JProtector

Java

3270/5250
Terminal-
und
Druckeremulation

Version 5.6

JProtector Benutzerhandbuch

Copyright

Copyright © 1986-2013 XPS Software GmbH

Alle Rechte vorbehalten.

Warenzeichen

Java ist ein Warenzeichen von Sun Microsystems, Inc.

InstallAnywhere ist ein Warenzeichen der Zero G Software, Inc.

Windows ist ein Warenzeichen der Microsoft Corporation.

MVS, OS/390, z/OS, VSE, VSE/ESA, VM/CMS, OS/400, TSO und CICS sind Warenzeichen der IBM Corporation.

Andere in diesem Handbuch erwähnten Marken- und Produktnamen sind Warenzeichen der jeweiligen Rechtsinhaber und werden hiermit anerkannt.

Inhaltsverzeichnis

Inhaltsverzeichnis **3**

Abbildungen **10**

Die Java Terminal- und Druckeremulation **13**

Allgemein 13

Features 13

Installation **14**

Allgemein 14

Installation als Applikation einer Version aus dem Internet 14

Installation als Appletversion von der Installations-CD 17

Installation als Java Web Start Version von der Installations-CD 18

Appletverwaltung **19**

Sessionverwaltung 19

Startupparameter 19

Spracheinstellung 20

Serverdatenbank berücksichtigen 20

Erzwungene Übernahme der Datenbank 20

Angabe der gewünschten Datenbank 20

Festlegung der Benutzerrechte 20

Information über den Aufruf als Java Web Start 21

Angabe des Java Web Start Ladeverzeichnisses 21

Angabe des Ladeverzeichnisses der JProtector Datenbasis 21

Helpdesk Funktionen 21

Angabe eines Verzeichnisses das erweiterte Filetransfer Definitionen enthält 21

Angabe der Puffergröße für den IND$File Transfer 21

Angabe über den Speicherort der JProtector Lizenzdatei 22

Angabe über den Speicherort der JProtector Datenbasis 22

Java Web Start 22

Einstieg **23**

Die Arbeitsoberfläche der Terminalemulation 23

Die Oberfläche einer Druckersession 24

Das JProtector Kontrollzentrum 25

Beschreibung der Funktionen der Werkzeugleiste 25

Erstellung einer neuen Session 26

Festlegung der Sessionparameter 27

Definition der TCP/IP Parameter 27

Vergabe eines Sessionnamens 28

Allgemeine Einstellungen **29**

Allgemeine Einstellungen - Allgemein 29

Mauszeiger bei der Texteingabe ausblenden ... 29
Datei mit Maskendefinitionen ... 29
Datei mit zusaetzlichen Werkzeugleisten ... 30
Standard Farbschema ... 30
Standard 3270 Tastaturbelegung ... 30
Standard 5250 Tastaturbelegung ... 30
Sprachen ... 30
Allgemeine Einstellungen – Erweitert ... 30
Doppelpufferung der Ausgabe unterdrücken ... 31
Tastatur nach Ausgabe vom Host immer freigeben ... 31
Ungültige Ausgabezeichen ignorieren ... 31
Modell bei ungültiger Ausgabeposition anpassen ... 31
Backspace Taste loescht nicht ... 31
Wiederhofunktion für gehaltene Interrupt Keys ... 31
Alarm bei der Hostausgabe unterdrücken ... 32
Eingabefokus bei Hintergrundausgabe holen ... 32
Bei Klick in SelPen Feld Eingabetaste ausloesen ... 32
Umschalt links beim Drücken verarbeiten 32
Allgemeine Einstellungen – Sessionmanager ... 32
Containermodus ... 33
Schliessen Button auf Reitern ... 33
Fensterposition fuer alle Models gleich ... 33
Tabulatorposition Model 2 ... 33
Single Signon ... 33
RACFBroker ... 33
Allgemeine Einstellungen – Query Reply ... 34
Allgemeine Einstellungen – Drucker ... 35
Standarddrucker ... 35
Host Code Page ... 35
Drucker Code Page ... 35
Automatische Druckererkennung ... 35
Screenshots auf Standard Systemdrucker ausgeben ... 36
Schema fuer farbige Screenshots ... 36
Allgemeine Einstellungen – Kontrollzentrum ... 36
Kontrollzentrum Modus aktiv ... 36
Session Statistiken sammeln ... 36
Kontrollzentrum automatisch verbergen ... 36
Informationen in der Detailansicht ... 37
Allgemeine Einstellungen – APIs ... 37
Ohio Klassenpfad Erweiterung ... 37
Pfad zur Datei xpshll.ini ... 37
HLLAPI Bridge Port ... 37
HLLAPI Bridge aktivieren ... 38
Entfernten HLLAPI Zugriff zulassen ... 38

Allgemeine Einstellungen – XPSDaemon Sicherheit 38
Schlüssellänge 38
Bei jedem Startup 38
Erzeuge neuen Schlüssel 39
Allgemeine Einstellungen – Telnet Sicherheit 39
Keystore mit Benutzerzertifikaten 39
Keystore Passwort 39
Keystore mit Zertifikaten vertrauenswürdiger Aussteller 40
Keystore Passwort 40
Allgemeine Einstellungen – Bearbeiten 40
Normal 40
Tabellenkalkulation - wortbezogen 40
Tabellenkalkulation - feldbezogen 41
Num. Vorz. nach vorne verschieben 41
Sessions 42
Allgemeines zu Sessions 42
Terminalsessions 42
Druckersessions 42
Erstellen einer neuen Session 43
Öffnen einer bestehenden Session 43
Sessioneinstellungen 44
Der Sessionverwaltungsdialog 44
Sessioneinstellungen - Typ 45
Sessioneinstellungen - TCP/IP 45
Hostname/Hostadresse(n.n.n.n) 46
Portnummer 46
Servletpfad 46
Sessioneinstellungen – Allgemein 47
Autostart 47
Reconnect 47
Mehrere Instanzen zulassen 47
Bildschirmmodell 47
Host Code Page 48
Tastaturbelegung 48
Startanwendung (nur XPSDaemon Sessions) 48
Sessioneinstellungen – Drucker 48
Zugeordneter Screenshot Drucker 49
Zugeordneter Host Drucker 49
Zugeordneten Host Drucker automatisch verbinden 49
Zugeordneter Host Drucker LU-Name/Pool-Name 49
Sessioneinstellungen – Konstanten 49
LU-Name/Pool-Name 50
Fixe Session ID 50

Fixe Session ID für zugeordneten Drucker 50
Sessioneinstellungen – Einfügemarke 50
Unterstrichen/Block 51
Blinkend 51
Fadenkreuz 51
Sessioneinstellungen – Ansicht 51
Zeichensatz Standard Bildschirmmodell / Zeichensatz Alternatives Bildschirmmodell 52
Blink-Attribut ignorieren 52
Farbschema 52
Sessioneinstellungen - 5250 52
Startmenü, Aktuelle Bibliothek, Benutzerprofil, Benutzerpasswort 52
Spaltentrenner 52
Sessioneinstellungen - Sicherheit 52
Serverauthentisierung verlangen 53
Zertifikat 53
Screenshots 54
Typ 54
Ausrichtung 54
Bereich 55
Ausgabe 55
Telnet SSL/TLS 56
Java Keystores 57
Client Keystore 57
Importieren der Informationen aus einer PKCS#12-Datei 57
Generieren eines privaten Schlüssels mit einem Zertifikatsrequest 58
Generierung eines privaten Schlüssels 58
Erstellung eines Zertifikatsantrags 59
Importieren der Ausstellerzertifikate sowie des Zertifikats für die Anwenderin 59
Trusted Keystore 60
Importieren des vertrauenswürdigen Ausstellerzertifikats 61
Digitale Zertifikate 62
Benutzerauthentisierung 63
Serverauthentisierung 64
Makros 67
Aufzeichnung eines Makros 67
Abspielen eines Makros 68
Der Makroverwaltungsdialog 69
Der Makroeditor 70
Beschreibung der Dialogfelder 71
Beschreibung der Editoren 71
Toolbarfunktionen 72
Fallbeispiel 73

Verfügbare Schritttypen 75

Tastaturbelegung 77

Der Verwaltungsdialog 77

Der Tastaturbelegungsdialog 78

Allgemein 78

Zuweisung einer Hosttaste 79

Andere Möglichkeiten der Tastaturbelegung 79

Tastenzuweisung – Hosttasten 79

Tastenzuweisung – Makros 80

Tastenzuweisung – Funktionen 80

Tastenzuweisung - Host Code Pages 80

Tastenzuweisung - Ohio Applets 81

Tastenzuweisung - Scripts 81

Tastenzuweisung - Sessions 82

Weitere Funktionen 82

Anzeige einer gedrückten Taste 82

Wiederherstellung der Standardbelegung 82

Auswahl der Tastatursprache 83

Anzeige der aktiven Zuordnungen 83

Aktuelle Zuordnungen - Hosttasten 83

Aktuelle Zuordnungen – Makros 83

Aktuelle Zuordnungen – Funktionen 84

Aktuelle Zuordnungen - Host Code Pages 84

Aktuelle Zuordnungen – Ohio Applets 84

Aktuelle Zuordnungen – Scripts 85

Aktuelle Zuordnungen – Sessions 85

Farbschemata 86

Der Verwaltungsdialog 86

Der Farbschemadialog 87

Farbauswahl 87

Emulationsrahmen in 3D 87

Freier Emulationsbereich = Hintergrund 87

Farbauswahl 88

Standardfarben 88

Ohio/Oska 89

Ausführung von Applets 89

Ohio Anzeigemodus 90

Skripts 91

Groovy 92

JavaScript 92

JRuby 92

Jython 93

Einblendung der Systemkonsole....93
Ausführung eines Skripts....93
Verwaltung der History-Liste....93

Konfigurierbare Werkzeugleisten....95

Separator....96
Syntax....96
Hostkey....96
Syntax....96
Makro....97
Syntax....97
Ohio....98
Syntax....98
Skript....99
Syntax....99

Drucker....101

Der Verwaltungsdialog....102
Druckertypen....102
Gerätekontext Drucker....102
Datei Drucker....103
Dokumententyp Drucker....103
Der Druckerdialog....103
Gerätekontext Drucker....103
Datei Drucker....106
Dokumententyp Drucker....108

Hostdrucker Gruppen....113

Der Verwaltungsdialog....113
Hostdrucker....114
Virtueller Gerätename....114
Fixe Session ID....114
Zugeordneter Drucker....114
Sessions....115
TCP/IP....115

IND$ - Filetransfer....116

Profiles....116
Transferdefinitionen....117
Transferlisten....118
Externe Transfers....119
Verlauf....120

Maskendefinitionen....121

Maskendefinition....121
Bildschirmmaske identifizieren....122
Definition von HotSpots....123

Single Signon 124
Verwaltung 125
Sonstiges 127
Live Update 127
Systeminformation 127
Informationen über den Benutzer 127
Informationen über die verwendete Java Virtual Machine 128
Informationen über das Betriebssystem 128
Informationen über die Applikation 128
Helpdesk 128
Erstellung einer Secure Token Datei 128
Verwendung eines Secure Token 129
Nachrichten 131

Abbildungen

Abb. 1: Auswahl der Sprache **14**
Abb. 2: Auswahl des Installationsordners **15**
Abb. 3: Auswahl der Verknüpfungsposition **15**
Abb. 4: Auswahl der Java VM **16**
Abb. 5: Installationszusammenfassung **16**
Abb. 6: Abschluss der Installation **17**
Abb. 7: Das XPS Zertifikat **17**
Abb. 8: Die JProtector Arbeitsoberfläche **23**
Abb. 9: Druckersession **24**
Abb. 10: Kontrollzentrum – Icon View **25**
Abb. 11: Kontrollzentrum – Detailansicht **26**
Abb. 12: Startup - Sessiontyp **27**
Abb. 13: Startup - TCP / IP Parameter **27**
Abb. 14: Startup - Session speichern unter **28**
Abb. 15: Kontrollzentrum mit geöffneter Session **28**
Abb. 16: Allgemeine Einstellungen - Allgemein **29**
Abb. 17: Allgemeine Einstellungen - Erweitert **31**
Abb. 18: Allgemeine Einstellungen - Sessionmanager **32**
Abb. 19: JProtector im Sessionmanager-Modus **34**
Abb. 20: Allgemeine Einstellungen – Query Reply **34**
Abb. 21: Allgemeine Einstellungen - Drucker **35**
Abb. 22: Allgemeine Einstellungen - Kontrollzentrum **36**
Abb. 23: Allgemeine Einstellungen - Ohio **37**
Abb. 24: Allgemeine Einstellungen – XPSDaemon Sicherheit **38**
Abb. 25: Allgemeine Einstellungen – Telnet Sicherheit **39**
Abb. 26: Allgemeine Einstellungen - Bearbeiten **40**
Abb. 27: Allgemeine Einstellungen – Bearbeiten -Beispiel **41**
Abb. 28: Dialog zur Sessionauswahl **43**
Abb. 29: Sessionverwaltung **44**
Abb. 30: Sessioneinstellungen - TCP / IP **46**
Abb. 31: Sessioneinstellungen - Allgemein **47**
Abb. 32: Sessioneinstellungen - Drucker **49**
Abb. 33: Sessioneinstellungen - Konstanten **50**
Abb. 34: Sessioneinstellungen - Einfügemarke **51**
Abb. 35: Sessioneinstellungen - Ansicht **51**
Abb. 36: Sessioneinstellungen - 5250 ..... **52**
Abb. 37: Sessioneinstellungen - Sicherheit **53**
Abb. 38: Screenshot Optionen **54**
Abb. 39: Definition einer Telnet SSL / TLS Session **56**
Abb. 40: Verwaltung von Benutzerzertifikaten **63**
Abb. 41: Verwaltung von Ausstellerzertifikaten **64**
Abb. 42: Verwaltung von Serverzertifikaten **66**
Abb. 43: Makro speichern unter **68**
Abb. 44: Makroverwaltung **69**
Abb. 45: Makroeditor **71**
Abb. 46: Kontextmenü im Editor **72**
Abb. 47: Einfügen eines neuen Makroschritts **72**
Abb. 48: Auswählen der Einfügeposition **72**
Abb. 49: Das bearbeitete Makro **74**
Abb. 50: Nachfrage für die Texteingabe **74**
Abb. 51: Zuordnung der Funktion 'Makro – Texteingabe splitten' **74**
Abb. 52: Ergebnis der Aufzeichnung mit Split der Texteingabe **75**
Abb. 53: Verwaltung der Tastaturbelegungen **77**
Abb. 54: Tastaturbelegung 3270 ..... **78**
Abb. 55: Tastaturbelegung 5250 ..... **78**
Abb. 56: Tastenzuweisung - Hosttasten **79**
Abb. 57: Tastenzuweisung - Makros **80**
Abb. 58: Tastenzuweisung - Funktionen **80**
Abb. 59: Tastenzuweisung - Host Code Pages **81**

Abb. 60: Tastenzuweisung - Ohio Applets 81
Abb. 61: Tastenzuweisung - Scripts 82
Abb. 62: Tastenzuweisung - Sessions 82
Abb. 63: Aktuelle Zuordnungen - Hosttasten 83
Abb. 64: Aktuelle Zuordnungen - Makros 83
Abb. 65: Aktuelle Zuordnungen - Funktionen 84
Abb. 66: Aktuelle Zuordnungen - Host Code Pages 84
Abb. 67: Aktuelle Zuordnungen - Ohio Applets 84
Abb. 68: Aktuelle Zuordnungen - Ohio Applets 85
Abb. 69: Aktuelle Zuordnungen - Sessions 85
Abb. 70: Verwaltung der Farbschemata 86
Abb. 71: Farbschema – feste Farben 87
Abb. 72: Farbschema - HSB 88
Abb. 73: Farbschema - RGB 88
Abb. 74: Ohio Applet Auswahl 89
Abb. 75: Ohio Anzeigemodus 90
Abb. 76: Groovy Skript mit Ohio Funktionalität 92
Abb. 77: JavaScript Skript mit Ohio Funktionalität 92
Abb. 78: JRuby Skript mit Ohio Funktionalität 92
Abb. 79: Jython Skript mit Ohio Funktionalität 93
Abb. 80: JProtector - Konsole 93
Abb. 81: Skripts Verwaltung 94
Abb. 82: Druckermenü 101
Abb. 83: Verwaltung der Drucker 102
Abb. 84: Gerätekontext Drucker - Allgemein 103
Abb. 85: Gerätekontext Drucker - Vorschübe 104
Abb. 86: Gerätekontext Drucker – Kanäle 104
Abb. 87: Gerätekontext Drucker – Code Page 105
Abb. 88: Druckerauswahl - Allgemein 105
Abb. 89: Druckerauswahl – Seite einrichten 106
Abb. 90: Druckerauswahl - Aussehen 106
Abb. 91: Datei Drucker - Allgemein 106
Abb. 92: Datei Drucker – Code Pages 107
Abb. 93: Dokumententyp Drucker – Vorspanndaten 108
Abb. 94: Dokumententyp Drucker - Abspanndaten 108
Abb. 95: Dokumententyp Drucker – Druckerspezifische Hexadaten 109
Abb. 96: Dokumententyp Drucker - Zeichenersetzung 109
Abb. 97: Dokumententyp Drucker – Hostdaten Ersetzung 110
Abb. 98: Dokumententyp Drucker – Allgemein 110
Abb. 99: Dokumententyp Drucker - Steuerzeichen 111
Abb. 100: Dokumententyp Drucker - Kanäle 111
Abb. 101: Dokumententyp Drucker – Code Pages 112
Abb. 102: Verwaltung der Hostdrucker Gruppen 113
Abb. 103: Hostdrucker Gruppe –Hostdrucker 114
Abb. 104: Hostdrucker Gruppen - Sessions 115
Abb. 105: Hostdrucker Gruppen – TCP/IP 115
Abb. 106: IND$ Filetransfer - Profiles 116
Abb. 107: IND$ Filetransfer - Transferdefinition 117
Abb. 108: Transfer in Liste speichern 117
Abb. 109: IND$ Filetransfer - Transferlisten 118
Abb. 110: IND$ Filetransfer – Externe Transfers 119
Abb. 111: IND$ Filetransfer – Bearbeitung externer Transferdefinitionen 119
Abb. 112: IND$ Filetransfer - Verlauf 120
Abb. 113: Maskendefinitionsmodus 121
Abb. 114: Maske identifizieren 122
Abb. 115: HotSpot definieren 123
Abb. 116: HotSpot anzeigen 124
Abb. 117: Maskendefinition - Kontextmenü 125
Abb. 118: Single Signon Definition 125
Abb. 119: Verwaltung der Maskendefinitionen 126
Abb. 120: Systeminformationen - Benutzer 127
Abb. 121: Systeminformationen - Java 128
Abb. 122: Systeminformationen - Betriebssystem 128

Abb. 123: Systeminformationen - Applikation 128
Abb. 124: Menüpunkt für den Secure Token Generator 129
Abb. 125: Secure Token Generator 129
Abb. 126: Erweitertes Hilfemenü für den Helpdesk 129
Abb. 127: Eingabe des Passwortes für das Secure Token 130
Abb. 128: Beenden des Helpdesks 130

Kapitel

1

Die Java Terminal- und Druckeremulation

Allgemein

JProtector ist eine 3270/5250 Terminal- und Druckeremulation der XPS Software GmbH. Die Emulation ist in Java implementiert und kann somit plattformunabhängig als Applet oder Applikation eingesetzt werden. Darüber hinaus unterstützt JProtector die Java Web Start Technologie, die eine Synthese aus einer lokalen Installation und dem Einsatz als Applet darstellt.

Beginnend mit Version 5.5 benötigt JProtector zur Ausführung mindestens eine Java VM der Version 1.6.

JProtector unterstützt den Aufbau von Telnet SSL/TLS Verbindungen. Alternativ stehen im Zusammenspiel mit dem XPS eigenen Telnetserver XPSDaemon erweiterte Möglichkeiten zur Verfügung wie z. B. die Komprimierung der übertragenen Daten oder vielfältige Möglichkeiten zur Identifizierung des Emulationsklienten über die bloße Kenntnis der TCP/IP-Adresse hinaus.

Features

JProtector bietet alle relevanten Funktionen, die von einer modernen Terminal- und Druckeremulation erwartet werden. Die nachfolgende Auflistung enthält einen Auszug:

- Lokale Installation z. B. unter Win32 oder Linux (Plattenspeicherbdarf < 10 MB)
- Ausführung als Java Applet oder unter der Kontrolle von Java Webstart
- Komfortabler IND$-Filetransfer
- Drucken eines oder einer Sammlung mehrerer Screenshots
- Konfigurierbare Oberfläche mit der Möglichkeit der Einschränkung des Funktionsumfangs
- Aufzeichnen, Bearbeiten und Abspielen von Tastaturmakros
- Abspielen von Java Applets (Ohio) zur Automatisierung von Emulationsabläufen
- HLLAPI Bridge zur Nutzung von HLLAPI Programmen
- Anpassen der Tastaturbelegung über Drag und Drop
- Konfigurierbare Farbschemas (auf Sessionebene)
- Einfachstes Aktivieren von Telnet SSL/TLS
- Helpdeskfunktion zur Freischaltung gesperrter Funktionen durch autorisiertes Personal
- Sessionmanager-Modus mit Single-Signon und optionalem RACF/Interface (z/OS)

Kapitel

2

Installation

Allgemein

Die Installation von JProtector wird unter Verwendung von InstallAnywhere der Firma Zero G durchgeführt. Aktuelle JProtector Versionen können von der Internetseiten der XPS Software GmbH unter http://www.xps.biz/de/download/jprotector/index.php für verschiedene Plattformen heruntergeladen werden. Alternativ können CDs mit den Installationsdateien bei der XPS Software GmbH angefordert werden.

Installation als Applikation einer Version aus dem Internet

Nach dem Herunterladen der Installationsdatei für die gewünschte Plattform und eventuell notwendiger Entkomprimierung ist die Installation gemäß den Vorgaben der Zielplattform zu starten. Daraufhin erfolgt zunächst die Installationsvorbereitung durch InstallAnywhere. Nach Abschluss der Vorbereitungen wird der nachfolgende Dialog eingeblendet, in dem die Installationssprache selektiert werden kann.

Abb. 1: Auswahl der Sprache

Die verfügbaren Sprachen sind 'Deutsch' und 'English'. Nach Auswahl der Sprache ist die Installation durch Drücken der Schaltfläche 'OK' fortzusetzen.

Im Anschluss an die Einblendung eines erklärenden Dialogs ist der Installationsordner auszuwählen. Dazu wird der folgende Dialog eingeblendet:

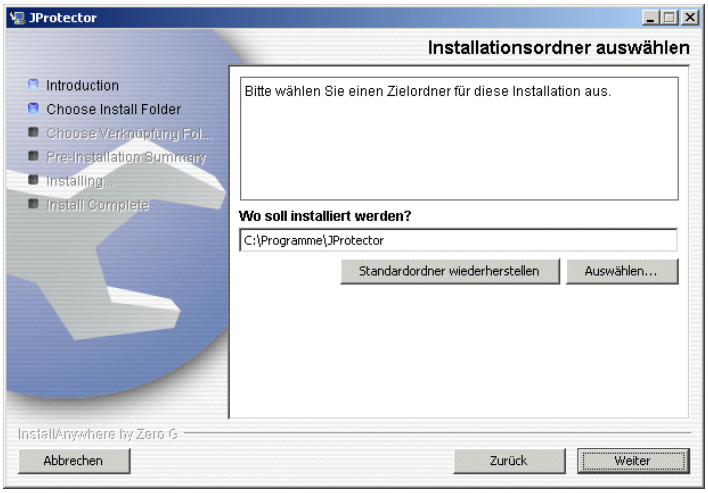


Abb. 2: Auswahl des Installationsordners

Wenn der vorgeschlagene Ordner nicht verwendet werden soll, kann durch Drücken der Schaltfläche 'Auswählen...' ein anderer Ordner für die Installation gewählt werden.

Nach Fortsetzung der Installation durch Auswahl der Schaltfläche 'Weiter' kann die Position für eine Verknüpfung mit JProtector festgelegt werden. Dazu wird der folgende Dialog verwendet:

Abb. 3: Auswahl der Verknüpfungsposition

Nachdem die Position für eine Verknüpfung festgelegt wurde, kann unter Verwendung der Schaltfläche 'Weiter' die Auswahl der Java Virtual Machine erfolgen, die zur Ausführung von JProtector genutzt werden soll.

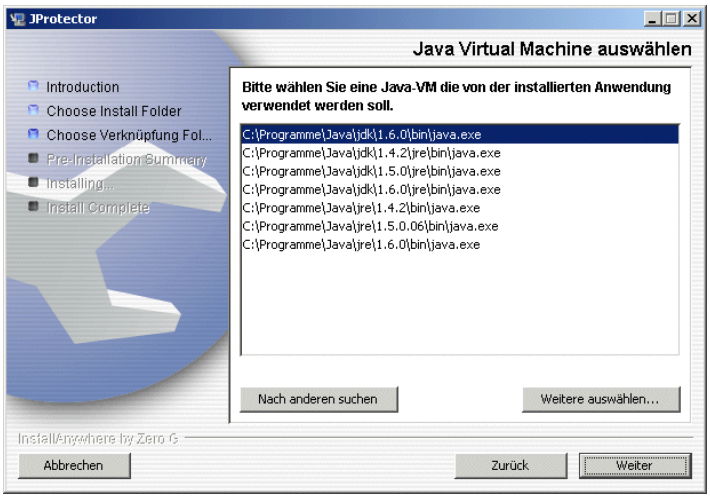


Abb. 4: Auswahl der Java VM

Es besteht die Möglichkeit, eine eigene Java VM für JProtector zu installieren oder eine bereits auf dem Betriebssystem installierte Java VM zu verwenden. JProtector benötigt ab der Version 5.5 zur Ausführung mindestens eine Java VM der Version 1.6!

Mit Auswahl der Java VM sind die Installationsvorbereitungen abgeschlossen. Zusammenfassend wird nun eine Dialogseite angezeigt, die eine Übersicht der gewählten Installationsoptionen enthält.

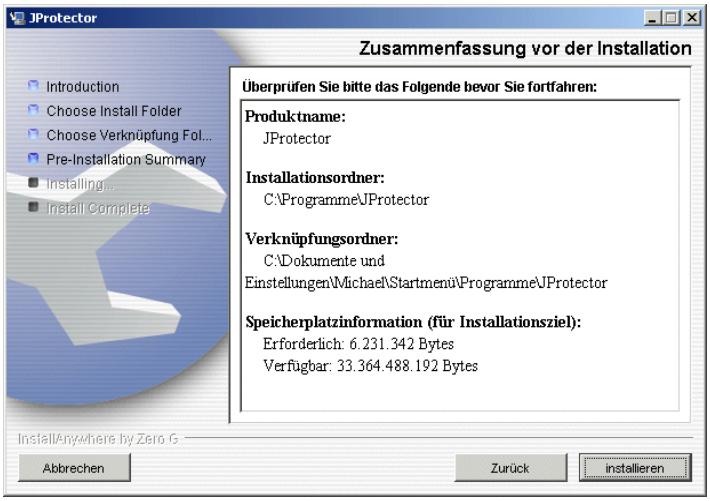


Abb. 5: Installationszusammenfassung

Schließlich ist die Installation durch Auswahl der Schaltfläche 'installieren' durchzuführen. Die erfolgreiche Durchführung der Installation wird durch das nachfolgende Bild angezeigt:

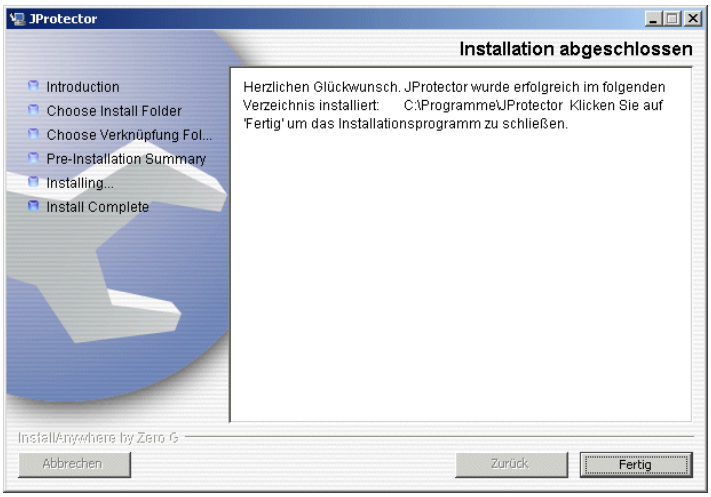


Abb. 6: Abschluss der Installation

JProtector steht nun zur Verwendung bereit.

Falls eine Programmverknüpfung erstellt wurde, kann die Emulation durch Aktivierung der erstellten Verknüpfung gestartet werden.

Informationen über den Einstieg in die Verwendung der Terminalemulation sind im Kapitel 'Einstieg' auf Seite 23 enthalten.

Installation als Appletversion von der Installations-CD

Die Installation der Appletversion erfolgt durch Kopieren der Dateien im Verzeichnis 'Applet\Image\' auf der Installations-CD in das gewünschte Zielverzeichnis auf dem Server.

Neben dem erforderlichen JProtector Java-Archiv enthält der Installationsordner zwei HTML-Dateien, mit deren Hilfe entweder ein deutsches oder englisches JProtector Applet gestartet werden kann.

Das JProtector Programmarchiv 'jprot.jar' benötigt zur Ausführung auf einem Clientrechner als Applet erweiterte Befugnisse, um z. B. eine TCP/IP Verbindung aufzubauen, oder um Einstellungen in der JProtector Datenbasis 'JProtector.xpsdb' zu speichern. Aus diesem Grund ist das Programmarchiv mit einem digitalen Zertifikat signiert. Beim Start des Applets muss der Benutzer darüber entscheiden, ob er dem JProtector Applet erweiterte Befugnisse erteilen möchte. Dies geschieht über den nachfolgend abgebildeten Dialog:

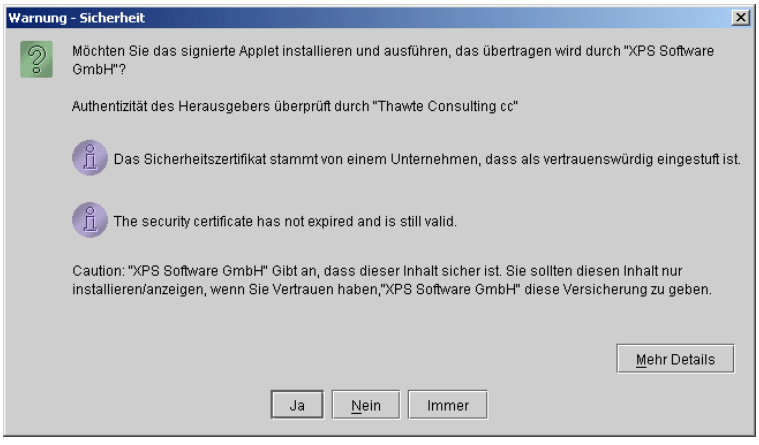


Abb. 7: Das XPS Zertifikat

Durch Auswahl von 'Ja' oder 'Immer ' werden dem JProtector Applet nur für diese eine Session oder für immer die erweiterten Befugnisse erteilt. Bei Auswahl von 'Nein' wird dies verhindert. In diesem Fall ist die Verwendung von JProtector nicht möglich. Nach Auswahl von 'Mehr Details' erfolgt die Anzeige weiterer Informationen über das digitale Zertifikat der XPS Software GmbH.

Installation als Java Web Start Version von der Installations-CD

Mit Hilfe der Java Web Start Technologie ist es möglich, die Vorteile einer lokal installierten Applikation mit den Vorteilen der zentralen Speicherung einer aktuellen Programmversion zu kombinieren. Die Voraussetzung für den Einsatz von JProtector unter Java Web Start ist, dass auf dem Client-Rechner Java Web Start installiert ist. Serverseitig ist es notwendig, den MIME Type 'JNLP' mit der Zuordnung 'application/x-java-jnlp-file' zu versehen. Nähere Informationen sind den Dateien 'readme.txt' sowie 'mimetype.txt' im Verzeichnis 'Webstart\' auf der Installations-CD zu entnehmen.

Die Installation der JProtector Web Start Version erfolgt durch Kopieren der Dateien im Verzeichnis 'Webstart\Image\' auf der Installations-CD in das gewünschte Zielverzeichnis auf einem Server.

Neben dem erforderlichen Java-Archiv zur Ausführung von JProtector enthält der Installationsordner zwei JNLP- und HTML-Dateien. Die JNLP-Dateien dienen zur Definition der erforderlichen Parameter für die Ausführung von JProtector unter Java Web Start. Die HTML-Dateien enthalten einfachen Code zum Starten von JProtector unter Verwendung eines HTML Browsers.

Kapitel

3

Appletverwaltung

JProtector stellt die Appletklasse 'JProtApplet.class' zur Verfügung. Bei der Installation der Appletversion auf einem Server werden HTML Dokumente kopiert, die einen Aufruf der JProtector Appletklasse enthalten. Die bei der Installation kopierten HTML Dokumente können selbstverständlich umbenannt und an firmeninterne Namenstandards angepasst werden.

Damit JProtector als Applet gestartet werden kann, ist es notwendig, dass der aufrufende HTML Browser mindestens das Java Plugin 1.6.0 installiert hat. Dazu enthalten die HTML Dokumente Javascript Code, der sicherstellt, dass das Plugin beim Start des Applets geladen, bzw. falls nicht vorhanden, installiert werden kann. Normalerweise erfolgt ein Download des Plugins von Oracle's Webseite. Neuere Versionen der Java VM installieren und registrieren sich automatisch als Browser Plugin.

Sessionverwaltung

Einer der Vorteile der Verwendung einer Appletversion liegt im geringen Verwaltungsaufwand. JProtector verwendet zum Speichern von Sessioneinstellungen eine Datenbank mit Namen 'JProtector.xpsdb'.

Der Administrator hat die Möglichkeit, im Installationsverzeichnis auf dem Server eine Standard JProtector Datenbank zu hinterlegen, die eine Reihe von Voreinstellungen für Sessions und die allgemeine Konfiguration von JProtector enthält.

Beim Aufruf eines der Benutzerapplets von einem Clientrechner aus wird jeweils geprüft, ob im Homeverzeichnis des Benutzers bereits eine JProtector Datenbank vorhanden ist. Wenn dies nicht der Fall ist, wird die vom Administrator erstellte Datenbank in das Homeverzeichnis des Benutzers kopiert. Andernfalls findet beim Appletstart eine Synchronisation der Datenbanken statt.

Das bedeutet, dass zum einen Sessions, die sich noch nicht in der Benutzerdatenbank befinden, aus der Serverdatenbank übernommen werden. Wenn darüber hinaus festgestellt wird, dass sich eine Session in der Serverdatenbank seit der letzten Übernahme in die Benutzerdatenbank verändert hat, wird die neuere Version aus der Serverdatenbank übernommen.

Startupparameter

Beim Startup von JProtector können verschiedene Einstellungen durch die Verwendung von Parametern vorgenommen werden. Die nachfolgend gewählte Notation zeigt die Parameterangaben beim Einsatz als Applet. Dieselben Parameter können auch bei der Nutzung von Java Web Start und beim Start als lokale Applikation über eine Kommandozeile bzw. in der Datei 'JProtector.properties' verwendet werden. In diesem Fall sind die Parameter in der jeweils geforderten Form anzugeben.

Spracheinstellung

```
<PARAM NAME="LANGUAGE" VALUE="de">
<PARAM NAME="COUNTRY" VALUE="DE">
```

Mit diesen beiden Parametern ist festzulegen, welche Ressourcendatei JProtector verwenden soll. Nach der Installation stehen HTML Dokumente bereit, die entweder deutsche oder englische Ressourcen verwenden.

Serverdatenbank berücksichtigen

```
<PARAM NAME="CONSIDER_SERVER_DB" VALUE="YES">
```

Bei der Erstellung einer Standarddatenbank durch einen Administrator ist es empfehlenswert, auf den Abgleich mit der aktuellen Serverdatenbank zu verzichten. Dazu ist dieser Parameter auf 'NO' zu setzen. Eine Serverdatenbank kann auch unter Verwendung einer JProtector Applikationsinstallation erstellt werden.

Erzwungene Übernahme der Datenbank

```
<PARAM NAME="FORCE_DB_DOWNLOAD" VALUE="YES">
```

In verschiedenen Situationen kann die Notwendigkeit entstehen, dass alle Benutzer mit einer neuen JProtector Datenbank vom Server versorgt werden sollen. Dies kann durch die Angabe von 'YES' zu obigem Parameter erzwungen werden. Wenn dieser Parameter gesetzt ist, wird jede Benutzerdatenbank, die ein Erstelldatum hat, das älter als das der Serverdatenbank ist, durch die Serverdatenbank ersetzt.

Angabe der gewünschten Datenbank

```
<PARAM NAME="DB_NAME" VALUE="JProtector.xpsdb">
```

Mit diesem Parameter kann festgelegt werden, welche JProtector Datenbank bei der Ausführung des Applets eingesetzt werden soll. Damit besteht die Möglichkeit, benutzergruppenabhängige Voreinstellungen festzulegen, die über verschiedene Applets aktiviert werden.

Festlegung der Benutzerrechte

```
<PARAM NAME="PERMISSIONS"
   VALUE="OPEN_SESSIONS,CREATE_SESSIONS,TRANSFER_FILES,ADMIN_SESSIONS,
          ADMIN_COMMON_PROPERTIES,OHIO_DEVELOPMENT,RECORD_MACROS">
```

Mit diesem Parameter kann der bereitgestellte JProtector Funktionsumfang eingeschränkt werden. Bei Weglassen einer Angabe steht die entsprechende Funktion nicht zur Verfügung. Folgende Optionen sind möglich:

OPEN_SESSIONS Durch die Angabe dieser Option wird es den Anwendern erlaubt, zuvor definierte Sessions zu öffnen, die nicht per Autostart automatisch gestartet werden.

CREATE_SESSIONS Durch die Angabe dieser Option wird es den Anwendern erlaubt, selbst neue JProtector Sessions zu erstellen.

TRANSFER_FILES Diese Option dient dazu, den Anwendern die Nutzung des IND$-Filetransfers zu ermöglichen.

ADMIN_SESSIONS Wenn diese Option gesetzt ist, können Benutzer Veränderungen an den JProtector Sessions vornehmen.

ADMIN_COMMON_PROPERTIES Damit ein Benutzer Veränderungen an den allgemeinen Einstellungen vornehmen kann, muss diese Option gesetzt sein.

OHIO_DEVELOPMENT Um Aktionen ausführen zu können, die im Zusammenhang mit der Entwicklung von Ohio Programmen notwendig sind, muss diese Option aktiviert sein.

RECORD_MACROS Damit Benutzer Tastaturmakros aufzeichnen können, muss diese Option aktiviert sein.

Information über den Aufruf als Java Web Start

```
<PARAM NAME="JAVA_WEBSTART" VALUE="NO">
```

Mit dieser Angabe ist JProtector darüber zu informieren, ob die Ausführung unter Kontrolle von Java Web Start erfolgt.

Angabe des Java Web Start Ladeverzeichnisses

```
<PARAM NAME="LOAD_LOCATION" VALUE=[PFAD]>
```

Angabe des vollständigen Pfades, in dem sich im Falle der Nutzung von Java Web Start die JProtector Dateien befinden.

Angabe des Ladeverzeichnisses der JProtector Datenbasis

```
<PARAM NAME="DB_STORE_LOCATION" VALUE=[PFAD]>
```

Mit dieser Angabe ist JProtector darüber zu informieren, in welchem Verzeichnis sich die JProtector Datenbasis befindet. Diese Angabe ist nur dann notwendig, wenn das von JProtector als Standard gewählte Verzeichnis nicht verwendet werden soll.

Helpdesk Funktionen

```
<PARAM NAME="SECTOKEN_GENERATOR" VALUE="YES">
<PARAM NAME="HELPDESK_SECTOKEN_FILE" VALUE=[PFAD]>
```

Durch die Möglichkeit, den Funktionsumfang für JProtector Anwender einzuschränken, könnte sich das Problem ergeben, dass auch der Helpdesk vor Ort nur die eingeschränkte JProtector Funktionalität nutzen kann. JProtector erlaubt durch den Einsatz von Secure Tokens, den Funktionsumfang beim Anwender bei Kenntnis eines Passwortes für das Secure Token temporär auf den maximalen Umfang zu erweitern und dann wieder einzuschränken.

Durch die erste Angabe wird dem Administrator die Möglichkeit eröffnet, Secure Tokens zu erstellen. Die zweite Angabe identifiziert ein Secure Token in einem Anwendungsszenario, das ein Administrator zur Freischaltung des JProtector Funktionsumfangs benutzen kann. Eine nähere Beschreibung erfolgt im Kapitel "Helpdesk" auf Seite 128.

Angabe eines Verzeichnisses das erweiterte Filetransfer Definitionen enthält

```
<PARAM NAME="FILETRANSFER_DIR" VALUE=[PFAD]>
```

JProtector unterstütz den IND$File Transfer. Dabei wird auch die Ausführung von Filetransfers, deren Definition sich in Textdateien befindet, ermöglicht. Diese Textdateien können entweder von Hand oder durch Generatoren erstellt werden. Näheres dazu ist dem entsprechenden Kapitel zu entnehmen. Mit der Angabe für diesen Parameter ist JProtector darüber zu informieren, welches Verzeichnis nach entsprechenden externen Filetransfer Definitionen durchsucht werden soll. Weitere Informationen sind dem Kapitel 'Externe Transfers' auf Seite 119 zu entnehmen.

Angabe der Puffergröße für den IND$File Transfer

```
<PARAM NAME="FILETRANSFER_SYSTEM_SIZE" VALUE=[WERT]>
```

Mit dieser Angabe kann die maximale Größe des Puffers festgelegt werden, den JProtector für die Übermittlung von Daten im Rahmen eines IND$File Transfers verwenden soll. Eine Angabe für diesen Wert überschreibt den im Rahmen der Initialisierung des File Transfers vom Host übermittelten Wert. Damit können eventuell auftretende Probleme, die sich aus der übermittelten Puffergröße ergeben, behoben werden.

Angabe über den Speicherort der JProtector Lizenzdatei

<PARAM NAME="LIC_FILE_FROM_JAR" VALUE="YES">

Mit dieser Angabe kann JProtector darüber informiert werden, dass sich die Lizenzdatei im Wurzelverzeichnis des JProtector Programmarchivs befindet. Diese Möglichkeit erleichtert die Verwaltung und Verteilung im Rahmen der Einbindung von JProtector in selbst entwickelte Produkte.

Angabe über den Speicherort der JProtector Datenbasis

<PARAM NAME="DB_FROM_JAR" VALUE="YES">

Mit dieser Angabe kann JProtector darüber informiert werden, dass sich die Datenbasis im Wurzelverzeichnis des JProtector Programmarchivs befindet. Diese Möglichkeit erleichtert die Verwaltung und Verteilung im Rahmen der Einbindung von JProtector in selbst entwickelte Produkte.

Java Web Start

JProtector unterstützt den Einsatz als Java Web Start Anwendung.

Java Web Start vereint die klassischen Vorteile von Applets und lokal installierten Applikationen. Beim ersten Start von JProtector von einer Serverlokation erzeugt Java Web Start eine lokale Kopie der benötigten JProtector Klassenbibliotheken auf dem Clientrechner. Bei jedem nachfolgenden Start von JProtector wird dann von Java Web Start automatisch geprüft, ob sich auf dem Server neuere Kopien der Klassenbibliotheken befinden. Wenn dies der Fall ist, werden diese Bibliotheken automatisch auf den Clientrechner herunter geladen.

Damit bietet der Einsatz von Java Web Start dieselben Vorteile wie der Aufruf eines Applet aus einem Webbrowser heraus - Aktualität der eingesetzten Version bei zentralem Ressourcenmanagement.

Darüber hinaus bietet Java Web Start dem Anwender aber weit größere Flexibilität bei der Verwendung von JProtector.

JProtector kann, wie ein Applet, über eine HTML-Seite aus einem Webbrowser heraus gestartet werden. Der entscheidende Vorteil in diesem Fall ist, dass JProtector nicht unter der Kontrolle eines vom Webbrowser geladenen Plugins läuft, sondern unter der Kontrolle einer browserunabhängigen Java Virtual Machine. Diese wird vom Browser als lokale Applikation gestartet. Damit wirken sich nachfolgende Browseraktionen nicht auf JProtector aus. Selbst das Schließen des Browsers zieht keine Beendigung von JProtector nach sich. Das Verhalten ist in diesem Fall vergleichbar mit dem einer Applikation. Der Webbrowser findet ausschließlich beim Startup Verwendung.

Weiterhin ist zu erwähnen, dass der Start von JProtector auch über Desktopicons bzw. aus dem Java Web Start Kontrollzentrum heraus erfolgen kann. In diesem Fall entfällt der Einsatz eines Webbrowsers vollständig. Dennoch bleibt der weiter oben beschriebene Vorteil des automatischen Versionsmanagements erhalten.

Aktuelle Informationen zur Java Web Start Technologie finden sich auf den Webseiten von Sun Microsystems, z.B. unter 'http://java.sun.com/products/javawebstart/news.html'.

Auf der JProtector Installations-CD sind im Verzeichnis 'Webstart' Beispieldateien enthalten, mit denen der Einsatz von JProtector als Java Web Start Applikation erfolgen kann.

Kapitel

4

Einstieg

Dieses Kapitel soll einen leichten Einstieg in den Umgang mit JProtector vermitteln.

Voraussetzung ist, dass JProtector bereits auf der lokalen Workstation installiert ist, bzw. als Applet oder unter Java Web Start aufrufbar ist. Zur Verwendung einer sicheren XPS Verbindung ist es notwendig, dass XPSDaemon auf dem Zielrechner installiert ist, mit dem eine Verbindung hergestellt werden soll. Bei Aufbau der Verbindung mit einem Telnetserver können sowohl ungesicherte als auch SSL Verbindungen verwendet werden.

Zunächst folgt eine kurze, allgemeine Beschreibung der Arbeitsoberfläche der Emulation. Im Anschluss daran wird der Verlauf der ersten Anmeldung an einen Host exemplarisch durchgeführt.

Die Arbeitsoberfläche der Terminalemulation

Die nachfolgende Abbildung zeigt eine typische JProtector Arbeitsoberfläche:

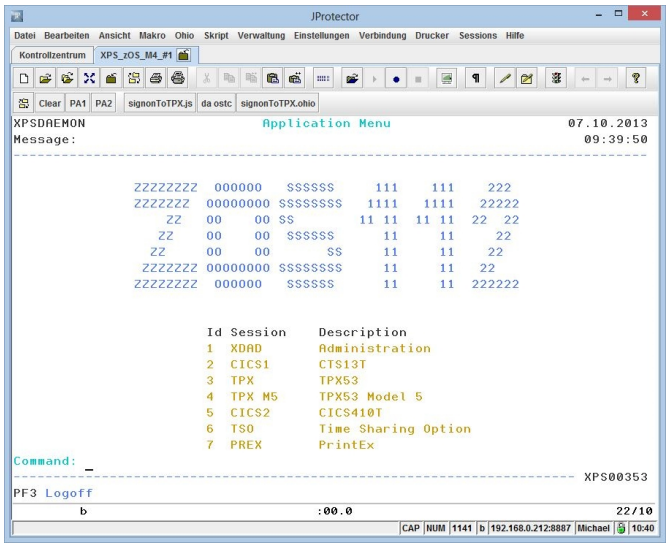


Abb. 8: Die JProtector Arbeitsoberfläche

Im oberen Teil des Fensters befinden sich das Menü und die Befehlsleiste. Die Befehlsleiste erlaubt einfachen Zugriff auf häufiger benötigte Funktionen. Zu den einzelnen Befehlsschaltflächen wird ein Tooltipp eingeblendet, wenn sich die Maus für eine kurze Zeit über der Schaltfläche befindet.

JProtector erlaubt die Definition weiterer, konfigurierbarer Befehlsleiste. Die Vorgehensweise hierzu ist in Kapitel 'Konfigurierbare Werkzeugleisten' auf Seite 95 beschrieben.

Die Statuszeile am unteren Rand enthält verschiedene Informationen, die über den momentanen Status der Emulation Aufschluss geben.

CAP/NUM	Aktueller Status der Caps- bzw. Num Lock Taste.
1141	Aktive Code Page zur EBCDIC / Unicode bzw. Unicode / EBCDIC Übersetzung.
b	Kurzbezeichnung für die Session für HLLAPI.
192.168…	IP Adresse des verbundenen Hosts.
Michael	Netzwerkname des Benutzers.
	Hinweis, dass die Datenübertragung für diese Session 128-Bit verschlüsselt erfolgt.
10:40	Aktuelle Uhrzeit.

Verschiedene Komponenten des JProtector Fensters können im Menü 'Ansicht' ein- bzw. ausgeblendet werden.

Hinweis: Für die Auswahl bestimmter Funktionen steht ein Popupmenü bereit, das mit Hilfe der rechten Maustaste über dem Emulationsfenster eingeblendet werden kann.

Die Oberfläche einer Druckersession

Die nachfolgende Abbildung zeigt eine Druckersession für den virtuellen Drucker TCPP1A05, der von XPSDaemon an der IP-Adresse 192.168.200.1:8887 reserviert wurde:

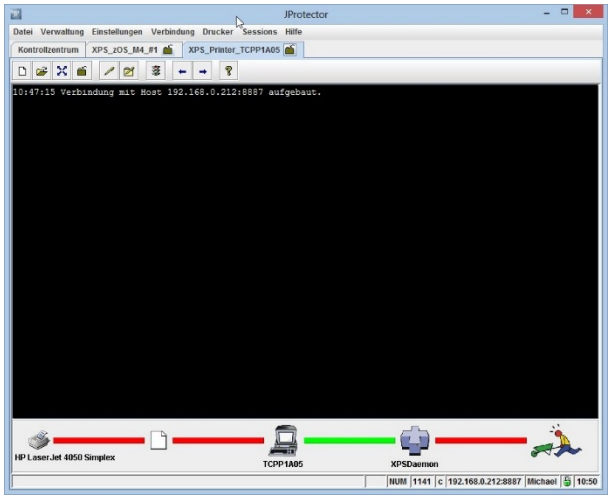


Abb. 9: Druckersession

Im unteren Bereich des Fensters ist ersichtlich, welche Teile der Verbindung zwischen physikalischem Drucker und kontrollierender Hostapplikation momentan aktiv sind (grün).

Sowohl das Menü als auch die Werkzeugleiste enthalten für eine Druckersession nur eine Teilmenge der Optionen, die für Terminalsessions verfügbar sind.

Das JProtector Kontrollzentrum

Nach dem ersten Start wird das JProtector Kontrollzentrum eingeblendet, von wo aus die zentrale Verwaltung von JProtector Sessions möglich ist.

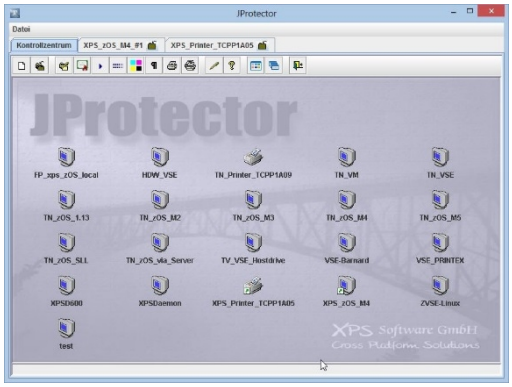


Abb. 10: Kontrollzentrum – Icon View

Beschreibung der Funktionen der Werkzeugleiste

Neu

Mit dieser Schaltfläche kann eine neue Session erstellt werden. Dazu wird der im Kapitel 'Sessioneinstellungen' ab Seite 44 beschriebene Dialog eingeblendet.

Alle Sessions schließen

Mit dieser Schaltfläche können alle geöffneten Sessions geschlossen werden.

Sessions verwalten

Mit dieser Schaltfläche kann der Dialog zur Verwaltung der Sessions eingeblendet werden.

Zertifikate verwalten

Mit dieser Schaltfläche kann der Dialog zur Verwaltung der X.509 Zertifikate eingeblendet werden.

Makros verwalten

Mit dieser Schaltfläche kann der Dialog zur Verwaltung der Tastaturmakros eingeblendet werden.

Tastaturbelegungen verwalten

Mit dieser Schaltfläche kann der Dialog zur Verwaltung der Tastaturbelegungen eingeblendet werden.

Farbschemata verwalten

Mit dieser Schaltfläche kann der Dialog zur Verwaltung der Farbschemata eingeblendet werden.

Ohio Applets verwalten

Mit dieser Schaltfläche kann der Dialog zur Verwaltung der Ohio Applets eingeblendet werden.

Drucker verwalten

Mit dieser Schaltfläche kann der Dialog zur Verwaltung der Drucker eingeblendet werden.

Allgemeine Einstellungen

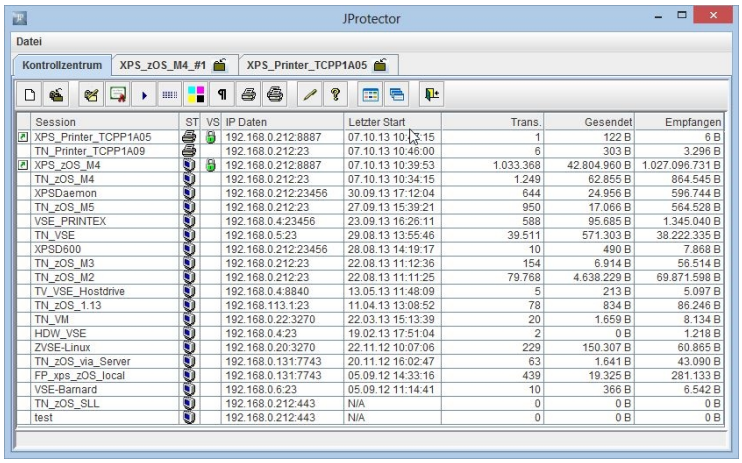
Mit dieser Schaltfläche kann der Dialog zur Verwaltung der allgemeinen Einstellungen eingeblendet werden.

Systeminformation

Mit dieser Schaltfläche kann der Dialog zur Anzeige der Systeminformationen eingeblendet werden.

Anzeigemodus ändern

Mit dieser Schaltfläche kann der Anzeigemodus des Kontrollzentrums verändert werden. Neben dem Icon View steht eine Detailansicht zur Verfügung. Die Detailansicht enthält einige statistische Angaben zu den einzelnen Sessions. Nach einem Rechtsklick mit der Maus in der Überschriftzeile der Liste wird ein Menü eingeblendet, mit dessen Hilfe die verschiedenen Spalten aus- bzw. eingeblendet werden können.



Session	ST	VS	IP Daten	Letzter Start	Trans.	Gesendet	Empfangen
XPS_Printer_TCPP1A05			192.168.0.212:8887	07.10.13 10:15	1	122 B	6 B
TN_Printer_TCPP1A09			192.168.0.212:23	07.10.13 10:46:00	6	303 B	3.296 B
XPS_zOS_M4			192.168.0.212:8887	07.10.13 10:39:53	1.033.368	42.804.960 B	1.027.096.731 B
TN_zOS_M4			192.168.0.212:23	07.10.13 10:34:15	1.249	62.855 B	864.545 B
XPSDaemon			192.168.0.212:23456	30.09.13 17:12:04	644	24.956 B	596.744 B
TN_zOS_M5			192.168.0.212:23	27.09.13 15:39:21	950	17.066 B	564.528 B
VSE_PRINTEX			192.168.0.4:23456	23.09.13 16:26:11	588	95.685 B	1.345.040 B
TN_VSE			192.168.0.5:23	29.08.13 13:55:46	39.511	571.303 B	38.222.335 B
XPSD600			192.168.0.212:23456	28.08.13 14:19:17	10	490 B	7.868 B
TN_zOS_M3			192.168.0.212:23	22.08.13 11:12:36	154	6.914 B	56.514 B
TN_zOS_M2			192.168.0.212:23	22.08.13 11:11:25	79.768	4.638.229 B	69.871.598 B
TV_VSE_Hostdrive			192.168.0.4:8840	13.05.13 11:48:09	5	213 B	5.097 B
TN_zOS_1.13			192.168.113.1:23	11.04.13 13:08:52	78	834 B	86.246 B
TN_VM			192.168.0.22:3270	22.03.13 15:13:39	20	1.659 B	8.134 B
HDW_VSE			192.168.0.4:23	19.02.13 17:51:04	2	0 B	1.218 B
ZVSE-Linux			192.168.0.20:3270	22.11.12 10:07:06	229	150.307 B	60.865 B
TN_zOS_via_Server			192.168.0.131:7743	20.11.12 16:02:47	63	1.641 B	43.090 B
FP_xps_zOS_local			192.168.0.131:7743	05.09.12 14:33:16	439	19.325 B	281.133 B
VSE-Barnard			192.168.0.6:23	05.09.12 11:14:41	10	366 B	6.542 B
TN_zOS_SLL			192.168.0.212:443	N/A	0	0 B	0 B
test			192.168.0.212:443	N/A	0	0 B	0 B

Abb. 11: Kontrollzentrum – Detailansicht

Sessionfenster kaskadieren

Mit dieser Schaltfläche können die geöffneten Sessionfenster kaskadiert, beginnend in der linken oberen Bildschirmecke angeordnet werden.

Diese Funktion kann ebenfalls über das 'Sessions'-Menü einer geöffneten Session ausgeführt werden.

Anwendung beenden

Mit dieser Schaltfläche kann das Kontrollzentrum geschlossen werden.

Erstellung einer neuen Session

Unter Verwendung der Schaltfläche ☐ können neue Sessions definiert werden. Es folgt eine kurze Beschreibung der wichtigsten Sessionparameter.

Festlegung der Sessionparameter

Zur Erstellung einer neuen Session wird der nachfolgend abgebildete Dialog verwendet:

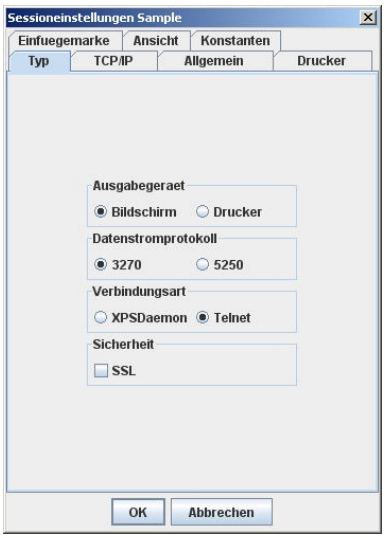


Abb. 12: Startup - Sessiontyp

Zunächst ist der Sessiontyp festzulegen. Dazu ist das gewünschte Ausgabegerät, das zu verwendende Datenstromprotokoll und die Verbindungsart auszuwählen. Schließlich kann für Telnet Sessions noch bestimmt werden, ob die Verbindung mit dem Host SSL-geschützt erfolgen soll. Bei Auswahl einer XPSDaemon Session ist dies immer der Fall.

Definition der TCP/IP Parameter

Nachdem der Sessiontyp festgelegt wurde, ist mit der Definition der TCP/IP Parameter fortzufahren. Dazu ist die nachfolgend abgebildete TPC/IP Dialogseite auszuwählen:

Abb. 13: Startup - TCP/IP Parameter

Durch Eingaben in diesen Dialog ist der Host festzulegen, mit dem eine Verbindung aufgebaut werden soll. Dazu ist die Angabe einer TCP/IP Adresse sowie einer Portnummer notwendig. Als Adresse kann entweder der Name eingegeben werden, unter dem der gewünschte Host im Netzwerk erreichbar ist. Wenn die TCP/IP Adresse bekannt ist, kann diese auch direkt verwendet werden.

Im Feld 'Portnummer' ist der TCP/IP Port festzulegen, über den der Datenaustausch zwischen JProtector und Host stattfinden soll. Für ungeschützte Telnet-Verbindungen ist im Allgemeinen die Portnummer 23 zu wählen.

Falls die Kommunikation über die XPS Serverkomponente XPSDaemon/Fireproof mit einem Host hinter einer Firewall erfolgen soll, können alternative Informationen für den Verbindungsaufbau angegeben werden.

Die weiteren Sessioneinstellungen können zu einem späteren Zeitpunkt erfolgen. Eine detaillierte Beschreibung erfolgt im Kapitel 'Sessioneinstellungen' auf Seite 44.

Vergabe eines Sessionnamens

Nach drücken der 'OK' Schaltfläche wird der Benutzer dazu aufgefordert, für die neu erstellte Session einen Namen zu vergeben. Dies geschieht mit Hilfe des nachfolgend abgebildeten Eingabedialogs:

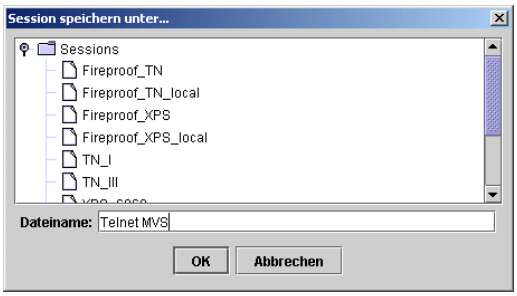


Abb. 14: Startup - Session speichern unter

Der gewählte Name wird von JProtector als Schlüssel zur Sessionidentifikation verwendet und in der Titelzeile des Emulationsfensters eingeblendet.

Nach Auswahl der Schaltfläche 'OK' ist die Sessiondefinition abgeschlossen und die neu erstellte Session wird im Kontrollzentrum angezeigt.

Die neu angelegte Session kann durch einen Doppelklick auf das Listenelement bzw. durch einen Klick auf das Icon im Icon View gestartet werden. In der Detailansicht wird die jeweils aktive JProtector Session in blauer Hintergrundfarbe angezeigt.

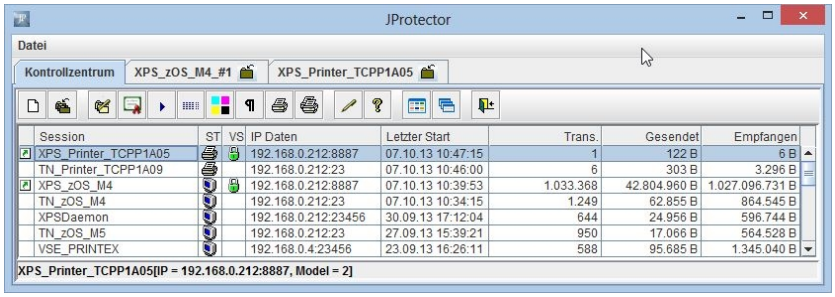


Abb. 15: Kontrollzentrum mit geöffneter Session

Kapitel

5

Allgemeine Einstellungen

In diesem Kapitel werden die allgemeinen JProtector Einstellungen erläutert. Allgemeine Einstellungen gelten für alle Sessions gleichermaßen.

Die allgemeinen Einstellungen werden mit Hilfe eines Dialoges verwaltet, der bei Auswahl des Menüpunktes 'Einstellungen::Allgemein' angezeigt wird.

Allgemeine Einstellungen - Allgemein

Die Seite 'Allgemein' des Dialogs sieht folgendermaßen aus:

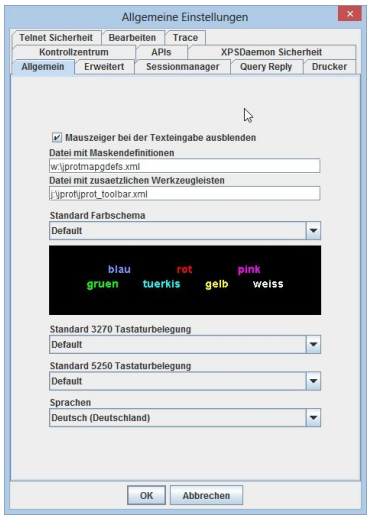


Abb. 16: Allgemeine Einstellungen - Allgemein

Mauszeiger bei der Texteingabe ausblenden

Wenn gewünscht ist, dass JProtector den Mauszeiger ausblendet, sobald der Anwender Text eingibt, ist diese Option zu selektieren. Der Mauszeiger wird, falls ausgeblendet, durch Bewegung der Maus wieder sichtbar.

Datei mit Maskendefinitionen

Zur Bereitstellung verschiedener Funktionen wie z. B. Single Signon, die die eindeutige Identifizierung von Bildschirmmasken erfordern, ermöglicht JProtector die Definition von Bildschirmmasken durch Auswahl eindeutiger Zeichenketten auf einer Maske.

Die auf diese Weise erstellten Maskendefinitionen werden in einem XML-Textformat abgespeichert. Mit dieser Option ist die voll qualifizierte Speicherstelle im Netzwerk bzw. die URL anzugeben, von der JProtector die Maskendefinitionen laden soll.

Durch Auswahl einer zentralen Speicherstelle können einmal erstellte Maskendefinitionen für mehrere JProtector Installationen bereitgestellt werden.

Eine Beschreibung der Vorgehensweise zur Erstellung von Maskendefinitionen sowie der möglichen Verwendung erfolgt im Kapitel 'Maskendefinitionen' auf Seite 121.

Datei mit zusaetzlichen Werkzeugleisten

Falls es gewünscht ist, unternehmensinterne, konfigurierbare Werkzeugleisten unter JProtector zu verwenden, können diese in einer externen Resourcendatei im XML-Format definiert werden. Mit Hilfe dieser Option ist der Speicherort der Konfigurationsdatei für weitere Werkzeugleisten bekannt zu geben.

Eine Beschreibung der Vorgehensweise zur Erstellung konfigurierbarer Werkzeugleistern erfolgt im Kapitel 'Konfigurierbare Werkzeugleisten' auf Seite 95.

Standard Farbschema

An dieser Stelle ist das Farbschema auszuwählen, das für neu erstellte Sessions standardmäßig verwendet werden soll. Mit Hilfe von Farbschemata kann die farbliche Gestaltung des Emulationsfensters festgelegt werden. Das Vorschaufeld unterhalb der Auswahlliste zeigt die Zuordnung der Farben, die für das ausgewählte Farbschema getroffen wurde.

Farbschemata können unter Verwendung des Menüpunktes 'Verwaltung::Farbschemata' definiert werden. Die Vorgehensweise ist in Kapitel 'Farbschemata' auf Seite **86** beschrieben.

Standard 3270 Tastaturbelegung

Mit dieser Auswahlliste kann festgelegt werden, welche Tastaturbelegung für neu erstellte 3270 Sessions verwendet werden soll.

Standard 5250 Tastaturbelegung

Mit dieser Auswahlliste kann festgelegt werden, welche Tastaturbelegung für neu erstellte 5250 Sessions verwendet werden soll.

Tastaturbelegungen können unter Verwendung des Menüpunktes 'Verwaltung::Tastaturbelegungen' definiert werden. Die Vorgehensweise wird im Kapitel 'Tastaturbelegung' auf Seite 77 beschrieben.

Sprachen

Mit dieser Auswahlliste kann festgelegt werden, welche Spracheinstellung bei der Anzeige von Fenstern und für die Ausgabe von Nachrichten von JProtector verwendet werden soll.

Allgemeine Einstellungen – Erweitert

Diese Dialogseite wird für die Durchführung spezieller Einstellungen verwendet. Einige dieser Einstellungen sollten nur unter besonderen Bedingungen aktiviert werden, die deren Einsatz notwendig machen.

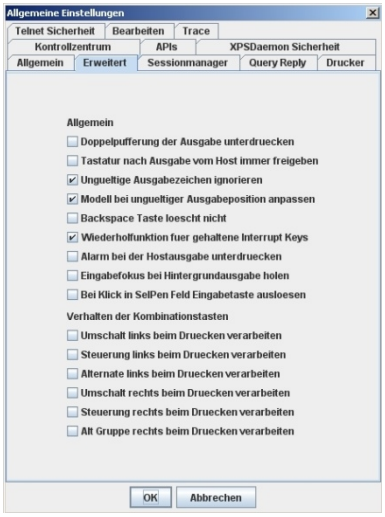


Abb. 17: Allgemeine Einstellungen - Erweitert

Doppelpufferung der Ausgabe unterdrücken

Eine Auswahl dieser Option hat zur Folge, dass JProtector den Bildschirmaufbau ungepuffert durchführt, womit deutliche Flackererscheinungen verbunden sind. Die Selektion dieser Option empfiehlt sich z. B. dann, wenn das Emulationsfenster auf einem X-Windows Client dargestellt wird. In diesem Fall kann die Deaktivierung der Doppelpufferung einen spürbaren Einfluss auf die Emulationsperformance haben.

Tastatur nach Ausgabe vom Host immer freigeben

Diese Option bewirkt, dass JProtector nach einer Ausgabe vom Host die Tastatur für neue Eingaben in jedem Fall freigibt, unabhängig davon, ob die vom Host gesendete Kontrolloption dies verlangt.

Ungültige Ausgabezeichen ignorieren

Bei Auswahl dieser Option wird die Einblendung eines 'ProgError' Fensters bei fehlerhaften Zeichen im Host Ausgabedatenstrom unterdrückt. Diese Option sollte nur gewählt werden, falls eine Korrektur der fehlerhaften Host Ausgabe nicht vorgenommen werden kann.

Modell bei ungültiger Ausgabeposition anpassen

Mit dieser Option wird bewirkt, dass JProtector das Terminal Modell automatisch anpasst, falls der Hostdatenstrom Positionsangaben enthält, die für das eingestellte Terminal Modell ungültig sind.

Backspace Taste loescht nicht

Mit dieser Option kann das Verhalten der Backspace Taste verändert werden. Selektion bewirkt, dass Zeichen, die links von der Cursorposition liegen, beim Linksverschieben des Cursors unter Verwendung der Backspace Taste nicht gelöscht werden.

Wiederhofunktion für gehaltene Interrupt Keys

Mit Auswahl dieser Option kann festgelegt werden, dass JProtector bei einer gehaltenen Interrupt Taste nach Ablauf eines kurzen Zeitintervalls den entsprechenden Host Interrupt erneut auslöst. Damit kann z. B. erreicht werden, dass bei gehaltener Taste für 'Vorwärts blättern' automatisch weitergeblättert wird, ohne dass die Taste erneut zu drücken ist.

Alarm bei der Hostausgabe unterdrücken

Durch Auswahl dieser Option kann die Berücksichtigung des eventuell hostseitig gesetzten 'Alarm'-Flags unterbunden werden.

Eingabefokus bei Hintergrundausgabe holen

Durch Auswahl dieser Option kann erreicht werden, dass eine JProtector Session, die sich im Hintergrund befindet und eine Ausgabe erhält, automatisch aktiviert und zur Vordergrundsession wird.

Bei Klick in SelPen Feld Eingabetaste ausloesen

Durch Auswahl dieser Option kann erreicht werden, dass JProtector bei einem Mausklick in ein Maskenfeld, das das Attribut 'Selector Pen detectable' enthält, das Auslösen der Datenfreigabetaste simuliert.

Umschalt links beim Drücken verarbeiten ...

Diese und die sich anschließenden verwandten Optionen dienen dazu, das Verhalten der Kombinationstasten Umschalt, Steuerung und Alternate anzupassen. Normalerweise verarbeitet JProtector diese Tasten erst, nachdem sie vom Benutzer losgelassen werden. Damit können die Kombinationstasten sowohl mit einer eigenen Funktion als auch mit einer Kombinationsfunktion belegt werden.

Wenn dies nicht erwünscht oder erforderlich ist, kann durch Auswahl der jeweiligen Option erreicht werden, dass die Taste bereits beim Drücken verarbeitet wird. Die Belegung der Taste mit einer Kombinationsfunktion ist dann allerdings nicht mehr möglich.

Allgemeine Einstellungen – Sessionmanager

Diese Dialogseite wird zur Festlegung der Optionen für den JProtector Sessionmanager-Modus verwendet. Im Sessionmanager-Modus werden alle geöffneten JProtector Sessions in einem gemeinsamen Fenster angezeigt.

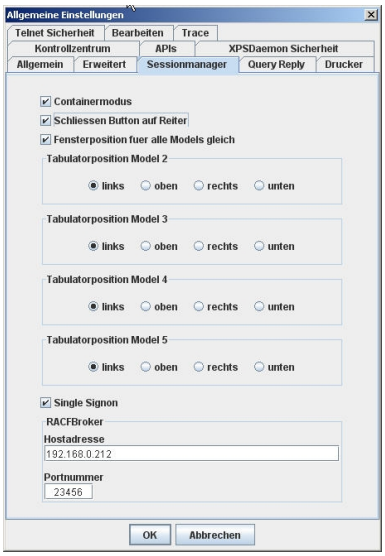


Abb. 18: Allgemeine Einstellungen - Sessionmanager

Containermodus

Eine Auswahl dieser Option hat zur Folge, dass JProtector alle Sessions in einem gemeinsamen Fenster, dem JProtector Container, darstellt. Mit Auswahl dieser Option wird dem Anwender die Übersicht über die jeweils aktuell die geöffneten Sessions erleichtert.

Schliessen Button auf Reitern

Wenn diese Option aktiviert wird, blendet JProtector auf dem Reiter jeder Session im Containermodus einen Button zu Schliessen der Session ein.

Diese und die fünf nachfolgenden Optionen sind nur bei aktivem Containermodus verfügbar.

Fensterposition fuer alle Models gleich

Wenn diese Option aktiviert wird, speichert JProtector die aktuelle Position des Containerfensters für alle Modelle ab. Damit wird verhindert, dass der Container seine Position auf dem Bildschirm verändert, wenn sich das angezeigte Terminalmodell verändert.

Tabulatorposition Model 2

Im Containermodus werden alle Sessions in einem Fenster mit einem gemeinsam genutzten Ausgabebereich dargestellt. Die einzelnen Sessions sind über die jeweils zugeordneten Reiter auszuwählen. Mit dieser und den drei nachfolgenden Optionen kann festgelegt werden, wo die Auswahlreiter jeweils platziert werden sollen, falls eine Bildschirmmaske des entsprechenden Modells angezeigt wird.

Single Signon

JProtector unterstützt die Verwendung von Single Signon. Dazu sind zunächst, wie in Kapitel 'Maskendefinitionen' auf Seite 121 beschrieben, alle Anmeldemasken eindeutig zu identifizieren und die Position der Eingabefelder für 'Name' und 'Passwort' bekannt zu geben.

Bei aktiviertem Single Signon Modus erfordert JProtector beim Start der Emulation eine Identifizierung des Anwenders durch die Eingabe eines Namens und eines Passwortes.

Wenn JProtector während der Verarbeitung eine der definierten Anmeldemasken identifiziert, werden die zuvor erfolgten Angaben für 'Name' und 'Passwort' automatisch in die Anmeldemaske eingespielt und das Drücken der Datenfreigabetaste simuliert. Damit erfolgt eine automatische Anmeldung des Benutzers an das jeweilige Subsystem.

RACFBroker

Unter z/OS ermöglicht JProtector die Nutzung der RACFBroker Funktionalität, die XPS auch als eigenständiges Produkt anbietet.

Dazu ist er erforderlich, dass auf einem vom Emulationsnutzer erreichbaren z/OS der RACFBroker/z von XPS installiert ist. Dieser kann entweder als eigenständige Applikation installiert werden oder als Option unter einer XPSDaemon Installation betrieben werden.

Falls der RACFBroker Modus aktiviert ist, gleicht JProtector die von Anwender eingegebenen Anmeldedaten sofort mit dem vom RACFBroker/z erreichbaren RACF auf Korrektheit und Gültigkeit ab. In diesem Fall kann der Anwender in Rahmen der Identifizierung durch Eingabe eines neuen Passwortes sowie dessen Bestätigung ein neues RACF Passwort setzen, wie dies z. B. auch bei der direkten Anmeldung an ein CICS möglich ist.

Mit den beiden Angaben für 'Hostadresse' und 'Portnummer' sind die TCP/IP Informationen bekannt zu geben, unter denen JProtector den RACFBroker/z erreichen kann.

Die nachfolgende Abbildung zeigt ein Beispiel für das Aussehen der JProtector Benutzeroberfläche im Sessionmanager-Modus:

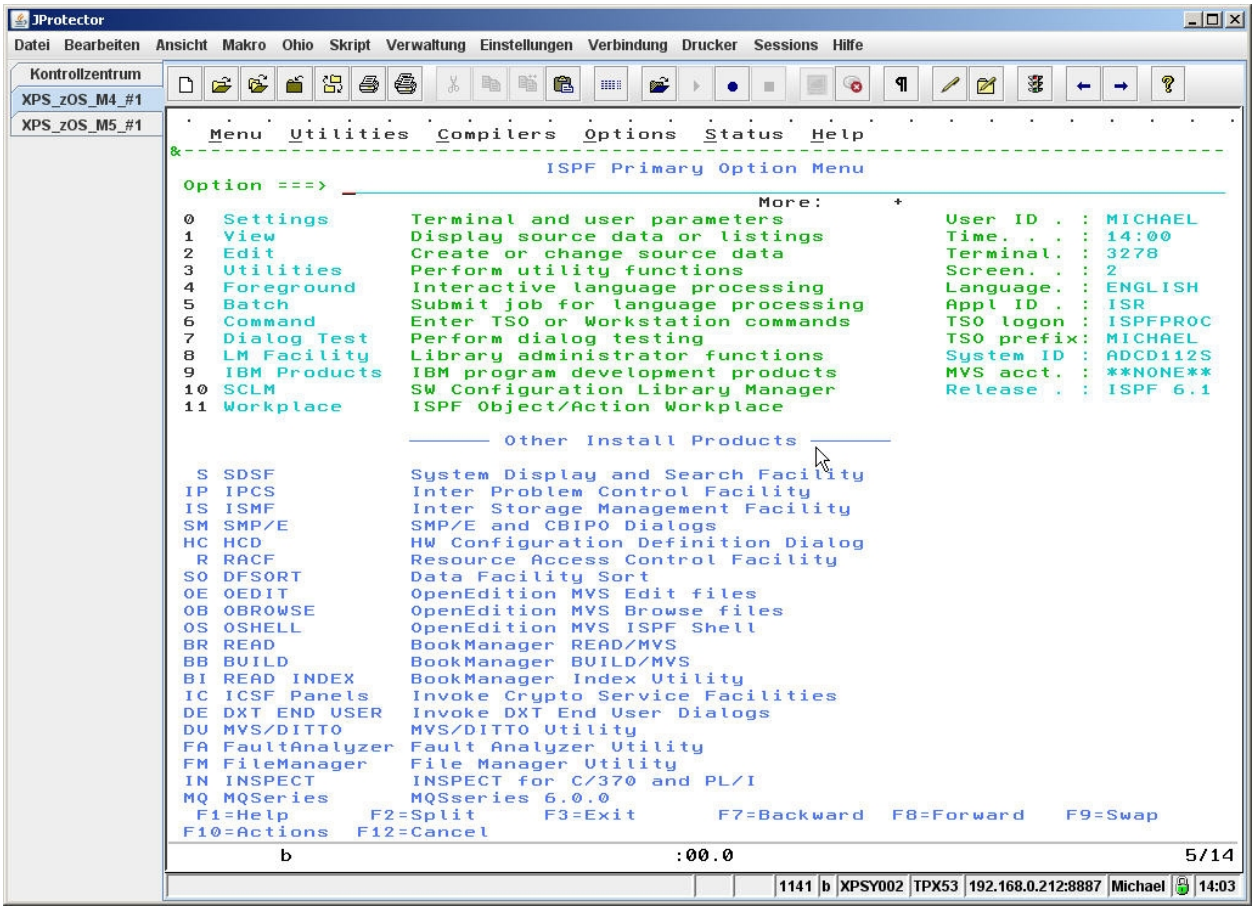


Abb. 19: JProtector im Sessionmanager-Modus

Allgemeine Einstellungen – Query Reply

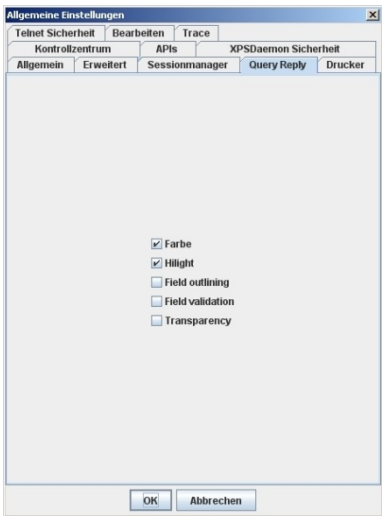


Abb. 20: Allgemeine Einstellungen – Query Reply

Verschiedene Hostanwendungen senden zu Beginn einer Session eine Anfrage an das angeschlossene Terminal, um sich über die Anzeigefähigkeiten des Terminals zu informieren. Dieser Prozess wird auch als 'Query Reply' bezeichnet.

Unter Auswahl der einzelnen Optionen auf dieser Seite kann festgelegt werden, welche Fähigkeiten zur Anzeige JProtector an die fragende Hostanwendung übermitteln soll.

Allgemeine Einstellungen – Drucker

Mit dieser Dialogseite können allgemeine Einstellungen im Zusammenhang mit den Druckfunktionen festgelegt werden.

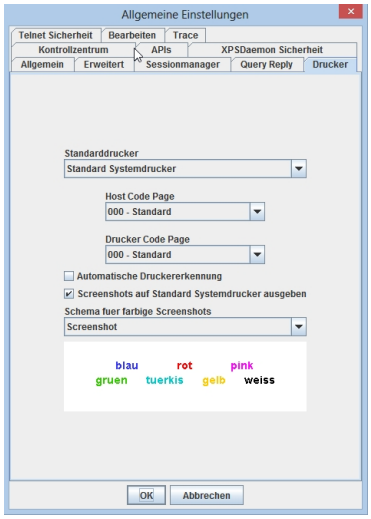


Abb. 21: Allgemeine Einstellungen - Drucker

Standarddrucker

Hier kann ein Drucker selektiert werden, der neu zu erstellenden Sessions automatisch zugeordnet wird.

Host Code Page

Mit diesem Kombinationsfeld kann festgelegt werden, welche Host Code Page Druckern zugeordnet werden soll, die von JProtector automatisch erkannt werden.

Drucker Code Page

Mit diesem Kombinationsfeld kann festgelegt werden, welche Drucker Code Page Druckern zugeordnet werden soll, die von JProtector automatisch erkannt werden.

Automatische Druckererkennung

Durch Aktivierung dieser Option kann JProtector angewiesen werden, den Arbeitsplatzrechner bei jedem Neustart der Emulation nach definierten Druckern zu durchsuchen. JProtector generiert in diesem Fall für alle nicht bereits definierten Drucker automatisch einen neuen Eintrag als Dokumententyp Drucker. Diese Drucker stehen dem Anwender dann sofort zur Auswahl als aktiver Drucker zur Verfügung.

Screenshots auf Standard Systemdrucker ausgeben

Durch Aktivierung dieser Option wird erreicht, dass Screenshots von JProtector – unabhängig vom Drucker, der der Session zugewiesen ist - immer auf den im System definierten Standarddrucker ausgegeben werden.

Schema fuer farbige Screenshots

Mit dieser Option ist das Farbschema auszuwählen, das zur Erstellung farbiger Screenshots verwendet werden soll. Die Definition und Verwaltung von Farbschemas ist in Kapitel 'Farbschemata' auf Seite 86 beschrieben.

Allgemeine Einstellungen – Kontrollzentrum

Mit dieser Dialogseite kann eingestellt werden, welche Spalten in der Detailansicht des Kontrollzentrums angezeigt werden sollen. Diese Einstellungen können auch mit Hilfe eines Menüs durchgeführt werden, das nach einem Rechtsklick mit der Maus auf die Überschriftzeile in der Detailansicht angezeigt wird.

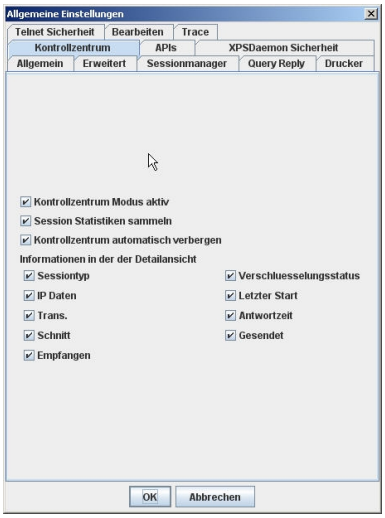


Abb. 22: Allgemeine Einstellungen - Kontrollzentrum

Kontrollzentrum Modus aktiv

Mit dieser Option kann die Verwendung des Kontrollzentrum Modus aktiviert bzw. deaktiviert werden.

Session Statistiken sammeln

Mit dieser Option kann entschieden werden, ob JProtector Statistiken über den Datenaustausch der jeweiligen Session sammeln soll oder nicht. Aus Performancesicht ist das Sammeln von Statistikinformationen vollkommen unkritisch.

Kontrollzentrum automatisch verbergen

Mit dieser Option kann festgelegt werden, dass JProtector das Kontrollzentrumsfenster automatisch ausblendet, sobald ein Sessionfenster angezeigt wird. Das Kontrollzentrumsfenster kann jederzeit durch Ausführen der Funktion 'Kontrollzentrum einblenden' wieder angezeigt werden, falls diese Funktion einer Tastenkombination zugeordnet wird.

Im Containermodus wird das Kontrollzentrum, falls aktiviert, immer als oberste Session geführt und ist somit nicht gesondert ein- bzw. auszublenden.

Informationen in der Detailansicht

Mit dieser Gruppe von Auswahlfeldern kann die Anzeige der jeweiligen Information in der Detailansicht aktiviert bzw. deaktiviert werden.

Allgemeine Einstellungen – APIs

Unter Verwendung dieser Dialogseite können Einstellungen vorgenommen werden, die im Zusammenhang mit den beiden von JProtector unterstützen APIs Ohio/Oska bzw. EHLLAPI von Bedeutung sind.

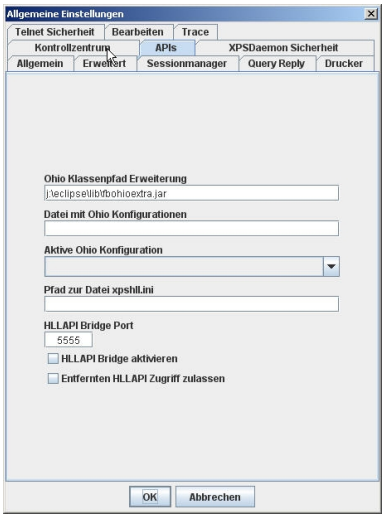


Abb. 23: Allgemeine Einstellungen - Ohio

Ohio Klassenpfad Erweiterung

Um ein Ohio/Oska Applet aus einer laufenden Terminalsession heraus zu starten, ist es erforderlich, JProtector über Archive zu informieren, die Ohio/Oska Applets enthalten. JProtector analysiert die angegebenen Archive in der Klassenpfad Erweiterung sowie den jeweiligen Java Klassenpfad und ermittelt die ausführbaren Applets. Weitere Erläuterungen zu Ohio/Oska sind dem Kapitel 'Ohio/Oska' auf Seite 89 zu entnehmen.

Pfad zur Datei xpshll.ini

Bei der Nutzung von HLLAPI erfolgt die Kommunikation zwischen JProtector und der externen MS-Windows Anwendung über eine zwischengeschaltete Windows DLL, deren Konfiguration in einer Datei namens 'xpshll.ini' abgespeichert wird.

In dieser Initialisierungsdatei wird u. a. der TCP/IP Port angegeben, über den die Kommunikation mit JProtector erfolgen soll. Diese Angabe kann zum Einen fest mit der nachfolgenden Option festgelegt werden. Zum anderen kann JProtector diesen Port auch aus der Datei 'xpshll.ini' lesen. Damit dies der Fall ist, ist mit dieser Option der Pfad zur Datei 'xpshll.ini' bekannt zu geben.

HLLAPI Bridge Port

JProtector unterstützt das 'EHLLAPI', das häufig zur Programmierung von Windowsbasierten Emulationen verwendet wird. Damit besteht die Möglichkeit, bestehende EHLLAPI Programme unter JProtector ohne Eingriff in die Programme weiter zu betreiben oder auch neue Programme zu erstellen. Die JProtector Implementierung von EHLLAPI basiert auf der Kommunikation mit einer Windows DLL über TCP/IP. Mit dieser Einstellung ist festzulegen, über welchen TCP/IP Port die EHLLAPI Kommunikation auf diesem Rechner abgewickelt werden soll.

HLLAPI Bridge aktivieren

Mit Hilfe dieser Option ist festzulegen, ob die JProtector EHLLAPI Bridge aktiviert werden soll. Falls dies nicht der Fall ist, eröffnet JProtector keinen TCP/IP Listener für den zuvor spezifizierten 'HLLAPI Bridge Port'.

Entfernten HLLAPI Zugriff zulassen

An dieser Stelle kann festgelegt werden, ob die JProtector HLLAPI Bridge auch von Programmen genutzt werden soll, die nicht auf demselben Rechner laufen, wie JProtector. JProtector analysiert jeweils die TCP/IP Adresse des Rechners, von dem aus ein HLLAPI Bridge Dienst angefordert wird. Falls diese Option nicht selektiert wird, und die Anforderung von einem fremden Rechner stammt, lehnt JProtector die Bearbeitung ab.

Allgemeine Einstellungen – XPSDaemon Sicherheit

XPSDaemon und JProtector tauschen beim Sessionaufbau ein Geheimnis aus: einen 128-Bit Blowfish Sessionschlüssel. Dieser Schlüssel wird, falls gewünscht, zur Verschlüsselung der übertragenen Sessiondaten eingesetzt. Zur Geheimhaltung dieses Sessionschlüssels erfolgt die Übertragung unter Verwendung der asymmetrischen Verschlüsselungsmethode RSA. An dieser Stelle ist festzulegen, woher das verwendete RSA Schlüsselpaar stammt. Zum einen besteht die Möglichkeit, dass JProtector RSA Schlüsselpaare erzeugt und verwaltet. Zum anderen kann ein RSA Schlüsselpaar aus einer PKCS#12 Datei entnommen werden, die ein digitales Zertifikat und einen privaten Schlüssel enthält. Die verfügbaren Optionen 'Schlüssellänge' und 'Schlüsselerzeugung' beziehen sich auf den Fall, dass RSA Schlüsselpaare von JProtector generiert werden.

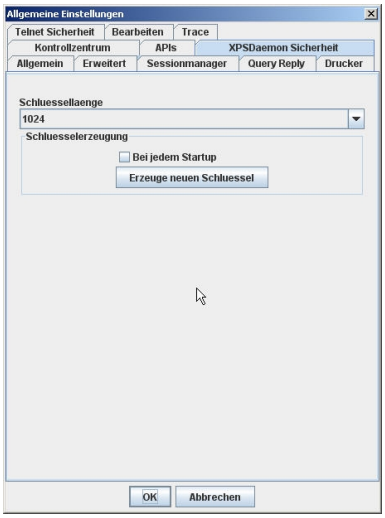


Abb. 24: Allgemeine Einstellungen – XPSDaemon Sicherheit

Schlüssellänge

Diese Auswahlliste dient zur Festlegung der Länge des erzeugten RSA Schlüsselpaares. Je größer die gewählte Schlüssellänge ist, desto schwieriger sind die damit verschlüsselten Daten zu korrumpieren. Allerdings vergrößert sich auch der benötigte Aufwand für Ver- und Entschlüsselung.

Bei jedem Startup

Wenn diese Auswahlbox selektiert ist, wird bei jedem JProtector Startup ein neues Schlüsselpaar erzeugt. Diese Auswahl sollte nur auf schnellen Rechnern aktiviert werden, da die Generierung eines RSA Schlüsselpaares durchaus einen merklichen Einfluss auf die Startup Performance von JProtector nimmt.

Erzeuge neuen Schlüssel

Wenn diese Schaltfläche gedrückt wird, erzeugt JProtector sofort ein neues RSA Schlüsselpaar.

Allgemeine Einstellungen – Telnet Sicherheit

JProtector ermöglicht die Verwendung SSL/TLS gesicherter Telnet Verbindungen mit einem Hostrechner. Wenn im Rahmen des Verbindungsaufbaus einer SSL/TLS Session keine Authentisierung erforderlich ist, genügt zur Aktivierung die Markierung des SSL-Kontrollkästchens im Rahmen der Sessiondefinition.

Falls Server- oder Clientauthentisierung – oder auch beides – erforderlich sind, dann sind die benötigten Daten auf der nachfolgend abgebildeten Dialogseite zu definieren.

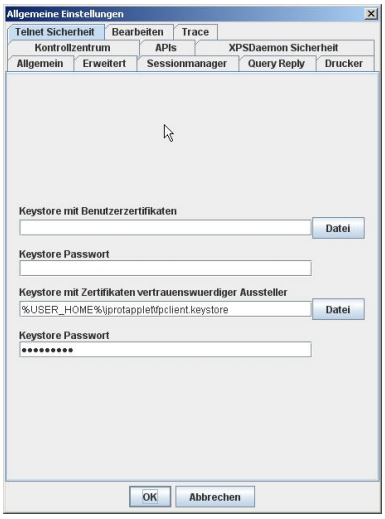


Abb. 25: Allgemeine Einstellungen – Telnet Sicherheit

Die Java Plattform verwendet so genannte 'Keystores' zur Verwaltung von digitalen Zertifikaten und privaten Schlüsselinformationen. Im Rahmen des Aufbaus einer SSL Verbindung, bei der ein gewisser Umfang an Authentisierung erforderlich ist, kommen diese Java Keystores zum Einsatz.

Ein Java Keystore ist mit Hilfe des Programmes 'keytool', das sich im Lieferumfang der Java Virtual Machine befindet, zu pflegen. Nähere Informationen zur technischen Vorgehensweise sind dem Kapitel 'Telnet SSL/TLS' auf Seite 56 zu entnehmen.

Keystore mit Benutzerzertifikaten

Seitens der Host Administration kann festgelegt werden, dass sich jeder Benutzer, der eine SSL Telnet Verbindung mit dem Host aufbauen möchte, durch Übermittlung eines digitalen Zertifikates authentisieren muss.

Zu diesem Zweck ist ein von Host akzeptiertes Benutzerzertifikat in einen Java Keystore zu importieren. Mit einer Angabe in dieses Eingabefeld wird JProtector über den Speicherort des Keystores informiert, aus dem der Java SSL Prozessor das Benutzerzertifikat entnehmen soll.

Die hier gemachte Angabe wird über den Java VM-Parameter **`'javax.net.ssl.keyStore='`** aktiviert.

Keystore Passwort

Der Zugriff auf den Keystore, der Benutzerzertifikate enthält, ist durch ein Passwort geschützt. Dieses Passwort ist JProtector in diesem Feld bekannt zu geben.

Diese Angabe wird über den Java VM-Parameter **'javax.net.ssl.keyStorePassword='** aktiviert.

Keystore mit Zertifikaten vertrauenswürdiger Aussteller

Damit der Client vom Host gesendetes Zertifikat akzeptiert, muss sich das Zertifikat des Ausstellers des Host Zertifikates in einem entsprechenden Java Keystore befinden. In diesem Eingabefeld ist der Pfad zum Java Keystore anzugeben, in dem alle akzeptierten und somit als vertrauenswürdig angesehenen Ausstellerzertifikate gespeichert sind.

Die Angabe wird über den Java VM-Parameter **'javax.net.ssl.trustStore='** aktiviert.

Keystore Passwort

Damit eine Java Anwendung auf Informationen zugreifen darf, die sich in einem Keystore befinden, muss das Passwort des Keystores bekannt sein. In diesem Feld ist das Passwort für den zuvor ausgewählten Keystore anzugeben.

Diese Angabe wird über den Java VM-Parameter **'javax.net.ssl.trustStorePassword='** aktiviert.

Allgemeine Einstellungen – Bearbeiten

Auf dieser Dialogseite kann festgelegt werden, auf welche Art und Weise JProtector Informationen aus einer Bildschirmmaske in die Zwischenablage des zu Grunde liegenden Betriebssystems kopiert.

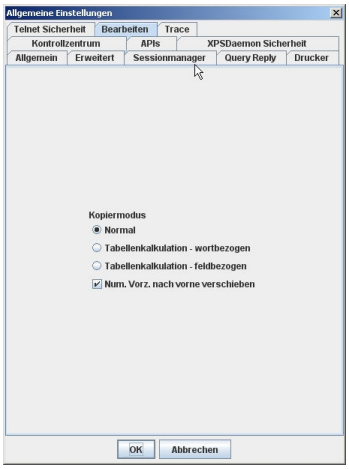


Abb. 26: Allgemeine Einstellungen - Bearbeiten

Normal

In diesem Modus analysiert JProtector die eingegebenen Daten nicht und erstellt ein Standardformat für die Zwischenablage.

Tabellenkalkulation - wortbezogen

In diesem Modus bricht JProtector den Inhalt des markierten Bereiches in einzelne, durch Leerzeichen getrennte, Worte auf, und stelle jedes resultierende Wort für eine Tabellenkalkulation als einen separaten Zellenwert bereit.

Tabellenkalkulation - feldbezogen

In diesem Modus bricht JProtector den Inhalt des markierten Bereiches in einzelne Felder auf, wie sie durch das Datenstromprotokoll vorgegeben sind, und stelle jeden resultierenden Feldinhalt für eine Tabellenkalkulation als einen separaten Zellenwert bereit.

Num. Vorz. nach vorne verschieben

In diesem Modus untersucht JProtector den markierten Bereich dahin gehend, ob nach dem Aufsplitten des markierten Bereichs gemäß einer der zuvor beschriebenen Optionen Zellenwerte mit nachgestellten Vorzeichen entstehen. Sollte dies der Fall sein und diese Option selektiert sein, verschiebt JProtector das nachgestellte Vorzeichen nach vorne.

Zur Veranschaulichung diene die nachfolgende abgebildete Markierung im PrintEx Editor von XPS, die in die Zwischenablage kopiert wird. Die jeweils hintereinander stehenden Werte befinden sich im selben Feld auf der Bildschirmmaske:

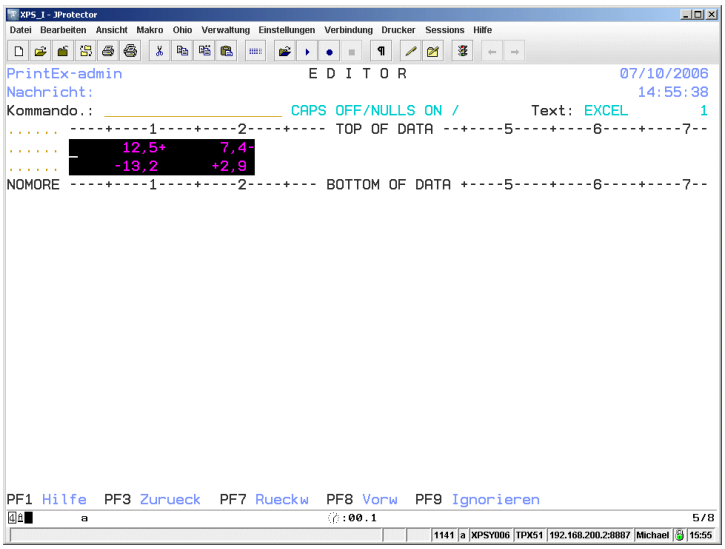


Abb. 27: Allgemeine Einstellungen – Bearbeiten -Beispiel

Folgende Ergebnisse ergeben sich bei Auswahl der unterschiedlichen Kopiermodi nach dem Einfügen in eine Tabellenkalkulation:

normal bzw. feldbezogen:

12,5+	7,4-	
-13,2	+2,9	

wortbezogen:

12,5+	7,4-	
-13,2	2,9	

wortbezogen und Vorzeichen nach vorne verschoben:

12,5	-7,4	
-13,2	2,9	

Kapitel

6

Sessions

Allgemeines zu Sessions

Unter einer JProtector Session ist genau eine TCP/IP Verbindung zwischen der Workstation und einem Hostrechner oder einem zwischengeschalteten Server zu verstehen. Dabei werden zwei verschiedene Arten von Sessions unterschieden.

Terminalsessions

Terminalsessions werden zur Anzeige von Bildschirmausgaben von Hostanwendungen verwendet. Dabei interpretiert JProtector den vom Host gesendeten Datenstrom und stellt ihn entsprechend der im Datenstrom enthaltenen Attribute und Positionierung dar.

Umgekehrt werden Benutzereingaben von JProtector in einen entsprechenden Datenstrom umgesetzt und zur Verarbeitung an den verbundenen Host gesendet.

Druckersessions

Druckersessions sind zur Verarbeitung von Druckausgaben von Hostapplikationen zu verwenden. Für die tatsächliche Druckausgabe stehen dem Benutzer dabei die Möglichkeiten zur Verfügung, die seine Systemumgebung bietet. Für die Druckausgabe kann ein Drucker gewählt werden, der entweder lokal an die Workstation angeschlossen ist oder über eine Netzwerkverbindung erreicht werden kann. Darüber hinaus kann die Druckausgabe auch in eine Datei zur weiteren Verarbeitung umgelenkt werden.

JProtector unterstütz die Verwendung von Druckersessions, die einer bestimmten Terminalsession zugeordnet sind. Für Telnet Sessions wird hierfür der Begriff 'ASSOCIATED Printer' verwendet. Im Rahmen der Konfiguration des Telnet Servers sind dazu Drucker und Terminal fest zu verknüpfen. Wenn der Benutzer dann während der Arbeit in einer Terminalsession entscheidet, dass er die zugeordnete Druckersession öffnen möchte (Menüpunkt 'Drucker::Verbinden) wird von JProtector im Hintergrund eine Session für den Drucker eröffnet, der dem Terminal zugeordnet wurde.

Damit entfällt die Notwendigkeit, eine separate Druckersession zu definieren und diese in einem eigenen Fenster zu starten. Unter Verwendung des Menüpunktes 'Ansicht::Umschalten' bzw. durch Klicken auf eines der Symbole oder in der Statuszeile kann zwischen der Ansicht der Terminal- und Druckersession umgeschaltet werden.

Eine Beschreibung zur Definition von Druckern befindet sich in Kapitel 'Drucker' auf Seite 101.

Erstellen einer neuen Session

Neue Sessions können unter Verwendung des Menüpunktes 'Datei::Neu' oder der Schaltfläche in der Werkzeugleiste erstellt werden. Daraufhin wird der Dialog zur Verwaltung von Sessioneinstellungen eingeblendet. Die einzelnen Dialogseiten sind im Kapitel 'Sessioneinstellungen' auf Seite 44 beschrieben. Nachdem die gewünschten Sessioneinstellungen vorgenommen worden sind, kann die Session unter einen frei wählbaren Namen in der JProtector Datenbasis gespeichert werden.

Öffnen einer bestehenden Session

Das Öffnen einer Session erfolgt unter Verwendung des Menüpunktes 'Datei::Öffnen', der Schaltfläche in der Werkzeugleiste oder durch die entsprechende Aktion im Kontrollzentrum. Im daraufhin eingeblendeten Dialog ist die zu öffnende Session auszuwählen.

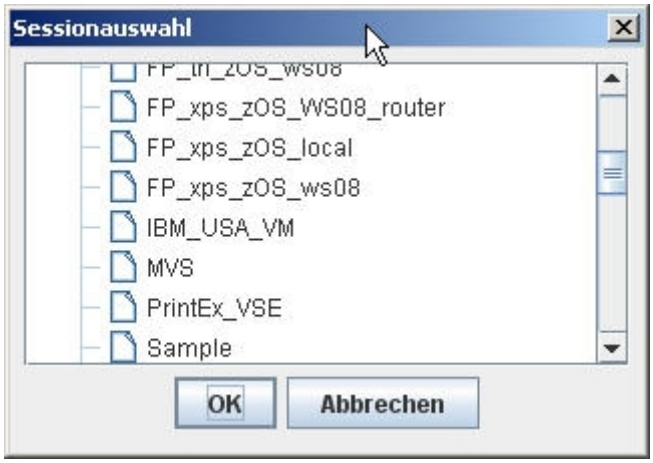


Abb. 28: Dialog zur Sessionauswahl

Kapitel

7

Sessioneinstellungen

In diesem Kapitel werden die Einstellungen beschrieben, mit deren Hilfe Sessions definiert werden.

JProtector ermöglicht dem Benutzer, beliebig viele Sessions parallel geöffnet zu haben. Dabei ist unter einer Session genau eine Verbindung zwischen einem Clientrechner und einem Host zu verstehen. Einzelne Sessions können unterschiedlich konfiguriert werden, um beispielsweise Besonderheiten einer Hostanwendung zu berücksichtigen.

Die Verwaltung nicht geöffneter Sessions erfolgt mit Hilfe des Menüpunktes 'Verwaltung::Sessions'. Geöffnete Sessions werden über den Menüpunkt 'Einstellungen::Session' verwaltet.

Hinweis: Der Umfang der vom Benutzer veränderbaren Sessioneinstellungen kann vom Systemadministrator eingeschränkt werden. Das bedeutet, dass eventuell nicht alle der nachfolgend beschriebenen Einstellmöglichkeiten für eine Session tatsächlich zur Verfügung stehen.

Der Sessionverwaltungsdialog

Die allgemeine Verwaltung von Sessions erfolgt mit Hilfe des Menüpunktes 'Verwaltung::Sessions' unter Verwendung des nachfolgend abgebildeten Dialogs:

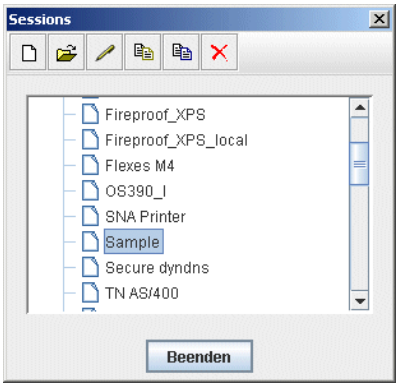


Abb. 29: Sessionverwaltung

Neu

Mit dieser Schaltfläche kann eine neue Session erstellt werden. Dazu kommt der im Folgenden beschriebene Dialog zum Einsatz.

Öffnen

Die ausgewählte Session kann unter Verwendung dieser Schaltfläche geöffnet werden. Bereits geöffnete Sessions können nicht erneut geöffnet werden!

Bearbeiten

Um Veränderungen an einer nicht geöffneten Session durchzuführen, ist die gewünschte Session in der Anzeige zu markieren und diese Schaltfläche zu betätigen. Veränderungen an der aktiven Session sind mit Hilfe des Menüpunktes 'Einstellungen::Session' durchzuführen.

Umbenennen

Die ausgewählte Session kann mit Hilfe dieser Schaltfläche umbenannt werden.

Kopieren

Kopieren der ausgewählten Session erfolgt unter Verwendung dieser Schaltfläche.

Löschen

Diese Schaltfläche erlaubt das Löschen der ausgewählten Session.

Sessioneinstellungen - Typ

Der Typ einer Session ist bei der Neuerstellung festzulegen. Eine Beschreibung befindet sich in Kapitel 'Einstieg' auf Seite 27.

Sessioneinstellungen - TCP/IP

Der Datenaustausch zwischen XPSDaemon und JProtector wird unter Verwendung des TCP/IP Protokolls durchgeführt.

Damit Host und Workstation miteinander kommunizieren können, ist es notwendig, dass die benötigte TCP/IP Verbindung eindeutig definiert ist.

Dazu dient die nachfolgend abgebildete Dialogseite, die auch beim ersten Startup von JProtector Verwendung findet.

Abb. 30: Sessioneinstellungen - TCP/IP

Hostname/Hostadresse(n.n.n.n)

Durch die Eingabe eines Hostnamens bzw. einer Hostadresse ist der Host zu identifizieren, mit dem die Session aufgebaut werden soll.

Als Eingabe ist entweder die vierstellige, numerische TCP/IP Adresse des Hosts anzugeben oder der Name, unter dem der Host im Netzwerk erreichbar ist.

Portnummer

XPSDaemon überwacht einen fest definierten TPC/IP Port des Hosts, auf dem er installiert ist. Über diesen Port müssen alle JProtector Clients die Verbindung mit XPSDaemon herstellen. Die Nummer des von XPSDaemon überwachten Ports ist in diesem Feld anzugeben.

Für Telnet Sessions ist die Portnummer anzugeben, die der Telnet Server überwacht. Im Allgemeinen ist dies die 23. Für Telnet SSL Sessions ist die zu verwendende Portnummer beim Administrator zu erfragen.

Servletpfad

Normalerweise schützen Firmen ihre internen Computernetzwerke durch Firewall-Programme. Um ein Höchstmaß an Sicherheit zu erlangen, wird dabei häufig der zulässige Datenübertragungsverkehr auf den HTTP Port 80 eines Gateway-Rechners eingeschränkt. Damit ist ein Hostrechner, der sich im geschützten Firmennetz befindet, von außen nicht mehr erreichbar. Dies kann in bestimmten Fällen aber durchaus gewünscht sein. Etwa für Außendienstmitarbeiter oder für Heimarbeitsplätze.

Im Zusammenspiel mit der Java-Serverkomponente XPSDaemon/Fireproof von XPS ermöglicht JProtector den Zugriff auf einen Host, der hinter einer Firewall verborgen ist. XPSDaemon/Fireproof ist ein Java Servlet, das dem Datenaustausch Client-Host zwischengeschaltet werden kann und die Möglichkeit bietet, den gesamten eingehenden Datenverkehr zum Host über TCP/IP Port 80 abzuwickeln.

Im Falle des Einsatzes von XPSDaemon/Fireproof ist mit Hilfe der TCP/IP Parameter Hostname/Hostadresse und Portnummer (i. a. 80) der Application- bzw. Webserver festzulegen, der das XPSDaemon/Fireproof Applet beheimatet. Zusätzlich ist in diesem Feld der Pfad anzugeben, unter dem das Servlet erreichbar ist. Das Format der Pfadangabe ist vom eingesetzten Application- bzw. Webserver abhängig.

Sessioneinstellungen – Allgemein

Allgemeinen Sessioneinstellungen können mit dem folgenden Dialog verwaltet werden:

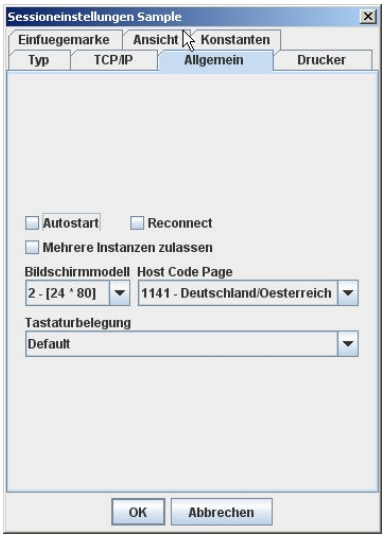


Abb. 31: Sessioneinstellungen - Allgemein

Autostart

Durch Aktivierung dieses Kontrollkästchens wird JProtector dazu veranlasst, die Session bei einem Startup automatisch zu starten. Wenn mehrere Autostart-Sessions definiert werden, erfolgt der Start in aufsteigender alphabetischer Reihenfolge der jeweiligen Sessionnamen.

Reconnect

Wenn gewünscht wird, dass die Session nach einer Unterbrechung bzw. nach einer Trennung vom Hostrechner automatisch neu verbunden wird, ist dieses Kontrollkästchen zu aktivieren.

Mehrere Instanzen zulassen

Wenn dieses Kontrollkästchen aktiviert wird, können beliebig viele Sessions mit der durchgeführten Definition gleichzeitig gestartet werden. Es ist zu beachten, dass durch diese Auswahl die Anzahl der möglichen Optionen für diese Session eingeschränkt wird. Insbesondere besteht nicht mehr die Möglichkeit, der Session Konstante, also z. B. einen bestimmten VTAM-LU-Namen, zuzuweisen.

Bildschirmmodell

Mit dieser Auswahlliste ist das Bildschirmmodell festzulegen, das für Hostausgaben im alternativen Format verwendet werden soll. Die Tabelle zeigt die verfügbaren Modelle.

Bildschirmmodell	Zeilen/Spalten
2	24/80
3	32/80
4	43/80
5	27/132

Hinweis: Der verwendete Zeichensatz lässt sich für das Standardmodell (2) und das gewählte alternative Bildschirmmodell separat einstellen. Dies erfolgt auf der Dialogseite 'Ansicht', deren Beschreibung weiter unten erfolgt.

Für 5250 Sessions stehen nur die Bildschirmmodelle '2' und '5' zur Auswahl.

Host Code Page

Die eingestellte Host Code Page wird von JProtector zur Umsetzung der vom Host erhaltenen Daten verwendet. Die folgende Tabelle zeigt jede mögliche Auswahl für diese Option:

Code Page	Länderkennung
1078	Portugal
1140	USA
1141	Deutschland/Österreich
1142	Dänemark/Norwegen
1143	Finnland/Schweden
1144	Italien
1145	Spanien
1146	England
1147	Frankreich
1148	Schweiz
1149	Island
1153	Osteuropa

Sollte die Darstellung einiger Zeichen der Hostmaske nicht richtig sein, besteht die Möglichkeit, dies durch Auswahl der passenden Code Page zu korrigieren.

Tastaturbelegung

Hier ist festzulegen, welche Tastaturbelegung von dieser Session verwendet wird. Die Verwaltung von Tastaturbelegungen ist im Kapitel 'Tastaturbelegung' auf Seite 77 beschrieben.

Startanwendung (nur XPSDaemon Sessions)

Dieses Feld dient zur Angabe einer Startanwendung für die Session und ist nur bei Sessions mit XPSDaemon verfügbar. Durch Angabe einer Startanwendung wird erreicht, dass XPSDaemon beim Aufbau der JProtector Session sofort eine Verbindung zur angegebenen Startanwendung herstellt.

Damit besteht zum Beispiel die Möglichkeit, dass sich der Benutzer nach erfolgtem Sessionaufbau direkt in einer CICS Umgebung befindet.

Sessioneinstellungen – Drucker

Drucker bezogene Einstellungen können mit dem folgenden Dialog verwaltet werden:

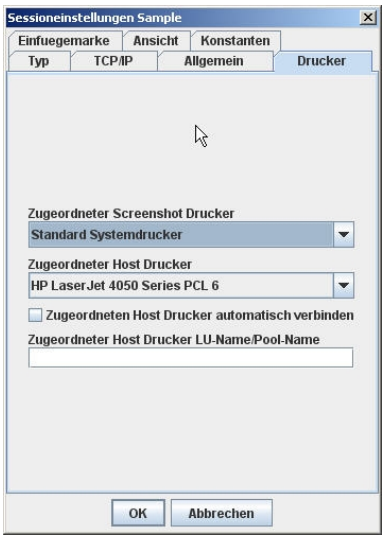


Abb. 32: Sessioneinstellungen - Drucker

Zugeordneter Screenshot Drucker

Hier ist festzulegen, welcher Drucker für diese Session verwendet werden soll um Screenshots zu drucken. Die Verwaltung von Druckern ist im Kapitel 'Drucker' auf Seite 101 beschrieben.

Zugeordneter Host Drucker

Hier ist festzulegen, welcher Drucker für diese Session verwendet werden soll um Hostausgaben zu drucken. Die Verwaltung von Druckern ist im Kapitel 'Drucker' auf Seite 101 beschrieben.

Zugeordneten Host Drucker automatisch verbinden

Mit dieser Schaltfläche ist darüber zu entscheiden, ob JProtector beim Start der Terminalsession automatisch versuchen soll, eine Verbindung mit einem eventuell zugeordneten Host Drucker aufzubauen (Telnet: ASSOCIATE, XPSDaemon: Druckerzuordnung im Rahmen der Benutzerverwaltung). Die Zuordnung eines Host Druckers zu einem Terminal erspart die separate Definition einer Druckersession.

Zugeordneter Host Drucker LU-Name/Pool-Name

Hier ist der LU- bzw. Pool-Name des Hostdruckers anzugeben, mit dem der virtuelle JProtector Drucker eine Verbindung aufbauen soll.

Sessioneinstellungen – Konstanten

JProtector ermöglicht die Vergabe von Konstanten, die für die Session immer zwingend zu verwenden sind. Damit besteht vor allem im Rahmen der Implementierung eines Logon-Exits unter XPSDaemon die Möglichkeit, einzelne Sessions an Hand der konstanten Definitionen eindeutig zu identifizieren.

Es ist zu berücksichtigen, dass das Sezen von Konstanten für eine Session nur dann erfolgen kann, wenn die Einstellung 'Mehrere Instanzen zulassen' in den allgemeinen Einstellungen für diese Session nicht aktiviert wurde.

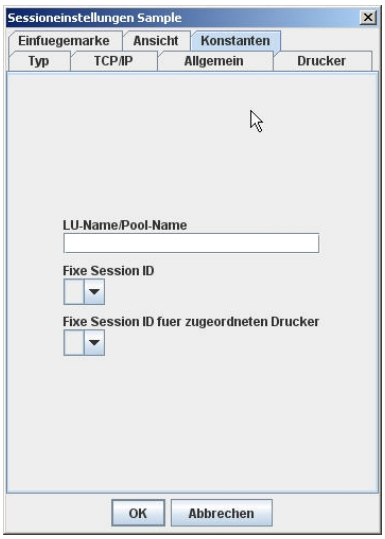


Abb. 33: Sessioneinstellungen - Konstanten

LU-Name/Pool-Name

In manchen Systemumgebungen ist es erwünscht oder erforderlich, dass einer Session in einem Hostsubsystem ein bestimmter virtueller VTAM LU-Name zugewiesen wird.

In diesem Eingabefeld ist der gewünschte virtuelle Gerätename festzulegen, der von JProtector im Rahmen des Verbindungsaufbaus an XPSDaemon oder an einen Telnetserver übermittelt wird.

Für reine Druckersessions ist diese Angabe notwendig.

Bei der Verwendung sicherer Sessions zwischen JProtector und XPSDaemon gibt es weitere Möglichkeiten für die Zuweisung eines LU-Namens zu einer Session. Da JProtector verschiedene Informationen über den Clientrechner an XPSDaemon übermittelt (z. B. Netzwerkname des Benutzers und Computername im Netzwerk) können diese Daten in einem Logon-Exit in XPSDaemon zur Ermittlung eines LU-Namens herangezogen werden. Weiterhin besteht die Möglichkeit, im Rahmen der XPSDeamon Online Benutzerverwaltung einzelnen Benutzern feste virtuelle Terminalnamen zuzuweisen-

Fixe Session ID

Falls gewünscht wird, dass die Session immer dieselbe fixe, einstellige Session ID erhalten soll, ist diese in diesem Auswahlfeld zu selektieren. JProtector übermittelt diese ID im Rahmen des Sessionaufbaus von sicheren Sessions an XPSDaemon, der diese Information im Logon-Exit zur Verfügung stellt.

Fixe Session ID für zugeordneten Drucker

Falls gewünscht wird, dass eine Druckersession, die der Terminalsession automatisch zugeordnet wird (associated printer) immer dieselbe fixe, einstellige Session ID erhalten soll, ist diese in diesem Auswahlfeld zu selektieren. JProtector übermittelt diese ID im Rahmen des Sessionaufbaus von sicheren Sessions an XPSDaemon, der diese Information im Logon-Exit zur Verfügung stellt.

Sessioneinstellungen – Einfügemarke

Die Einfügemarke zeigt die Maskenposition an, an der die nächste Texteingabe über die Tastatur erfolgt. Der Benutzer kann das Aussehen der Einfügemarke in gewissem Rahmen seinen Gewohnheiten anpassen. Dazu wird die nachfolgend abgebildete Dialogseite verwendet:

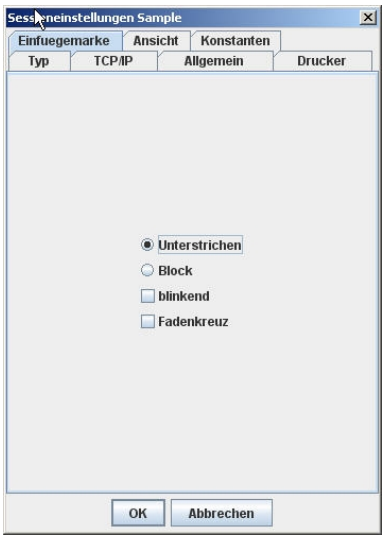


Abb. 34: Sessioneinstellungen - Einfügemarke

Unterstrichen/Block

Hier ist festzulegen, ob die Einfügemarke als Block oder lediglich als Unterstrich dargestellt werden soll. Bei Blockdarstellung erscheint die Position für die nächste Eingabe revers.

Blinkend

Die Markierung dieses Auswahlkästchens hat zur Folge, dass die Einfügemarke blinkt.

Fadenkreuz

Bei Auswahl dieser Einstellung wird ein Fadenkreuz über das Emulationsfenster eingeblendet, in dessen Schnittpunkt sich die Position der Einfügemarke befindet.

Sessioneinstellungen – Ansicht

Über die nachfolgend abgebildete Dialogseite kann das visuelle Erscheinungsbild einer Session konfiguriert werden.

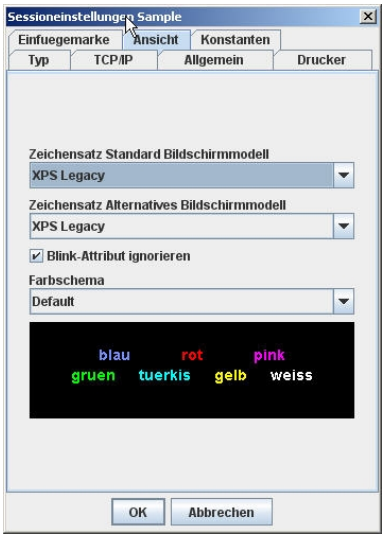


Abb. 35: Sessioneinstellungen - Ansicht

Zeichensatz Standard Bildschirmmodell / Zeichensatz Alternatives Bildschirmmodell

Die Festlegung des Zeichensatzes für das jeweilige Bildschirmmodell erfolgt über diese Auswahllisten. Zur Auswahl stehen die Zeichensätze 'Monospaced' und 'XPS Legacy'. Die Zeichensatzgröße ist durch Veränderung der Größe des Emulationsfensters mit Hilfe der Maus einzustellen. Auf Grund der besseren Les- und Skalierbarkeit wird der Einsatz des Zeichensatzes 'XPS Legacy' empfohlen.

Blink-Attribut ignorieren

JProtector unterstützt die Anzeige des Feldattributes 'blinkend'. Bei Auswahl dieser Option wird die Berücksichtigung dieses Attributes unterdrückt.

Farbschema

An dieser Stelle ist das Farbschema auszuwählen, das für die Darstellung des Emulationsfensters verwendet werden soll. Farbschemata werden in Kapitel 'Farbschemata' auf Seite 86 näher beschrieben.

Sessioneinstellungen - 5250

Mit Hilfe dieser Dialogseite können einige spezielle Sessionparameter für 5250 Sessions festgelegt werden.

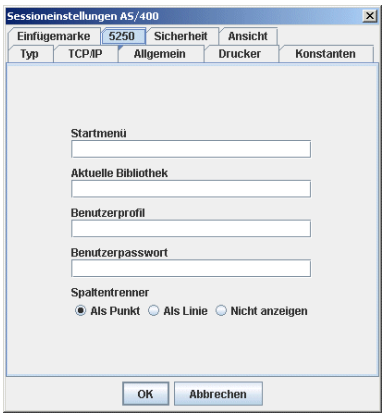


Abb. 36: Sessioneinstellungen - 5250

Startmenü, Aktuelle Bibliothek, Benutzerprofil, Benutzerpasswort

Eingaben in diese Felder können hostseitig zur Durchführung eines Auto-Signon an OS/400 verwendet werden. Diese Felder stehen nur für sichere XPSDaemon 5250 Sessions zur Verfügung.

Spaltentrenner

Aus den Vorgaben ist die gewünschte Darstellung des Spaltentrenners (column separator) auszuwählen.

Sessioneinstellungen - Sicherheit

Auf dieser Dialogseite können Sicherheitsoptionen für verschlüsselte JProtector Sessions mit XPSDaemon festgelegt werden.

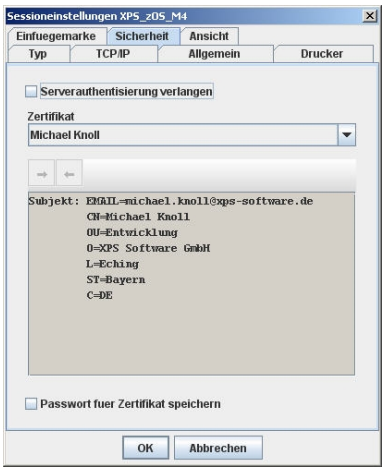


Abb. 37: Sessioneinstellungen - Sicherheit

Serverauthentisierung verlangen

Mit diesem Auswahlkästchen kann der Benutzer verlangen, dass sich das Hostsystem, mit dem eine Verbindung aufgebaut werden soll, durch ein X.509 Zertifikat authentisiert. Auf Grund der Tatsache, dass hierzu hostseitig eine RSA Entschlüsselung durchgeführt werden muss, ist zu bedenken, dass diese Auswahl den Verbindungsaufbau merklich verlangsamen kann.

Zertifikat

Hier ist ein Zertifikat auszuwählen, das JProtector im Rahmen des Verbindungsaufbaus an XPSDaemon zur Authentisierung des Benutzers senden soll.

Sollte die gewählte PKCS#12 Datei neben dem Benutzerzertifikat auch Ausstellerzertifikate enthalten, sind die Schaltflächen 'Nächstes in Kette' und 'Vorheriges in Kette' aktiviert. Mit diesen Schaltflächen kann durch die Zertifikatkette navigiert werden.

Die Zuweisung von Zertifikaten auf Sessionebene ermöglicht die Verwendung verschiedener Zertifikate, was sich bei der Arbeit mit mehreren Hostrechnern als vorteilhaft erweisen kann.

Vor der Verwendung zur Benutzerauthentisierung sind die gewünschten X.509 Zertifikate in die JProtector Datenbasis zu importieren. Die notwendige Vorgehensweise ist im Kapitel 'Digitale Zertifikate' auf Seite 62 beschrieben.

Kapitel

8

Screenshots

Die Erstellung eines Screenshots mit JProtector erfolgt durch Anklicken des Auswahlknopfes aus der JProtector Standard Werkzeugleiste oder durch Drücken einer Tastenkombination die im Rahmen der Konfiguration der Tastaturbelegung mit der Erstellung eines Screenshots verknüpft wurde.

Nach Auswahl der Funktion wird der nachfolgend abgebildete Dialog eingeblendet:

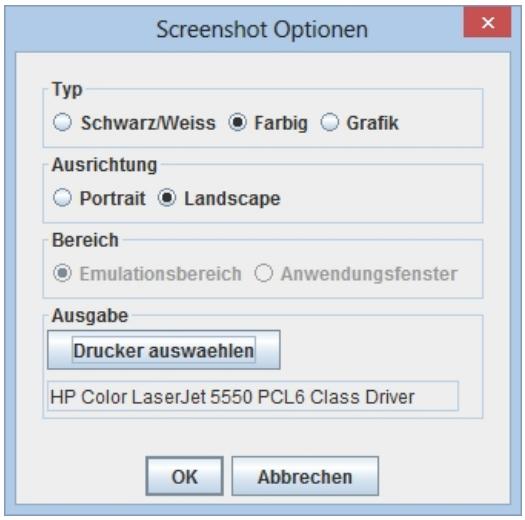


Abb. 38: Screenshot Optionen

Der Dialog wird beim Aufruf mit den zuletzt gewählten Einstellungen vorbelegt, so dass nur im Falle einer Änderung andere Optionen auszuwählen sind.

Die folgenden Optionen können gewählt werden:

Typ

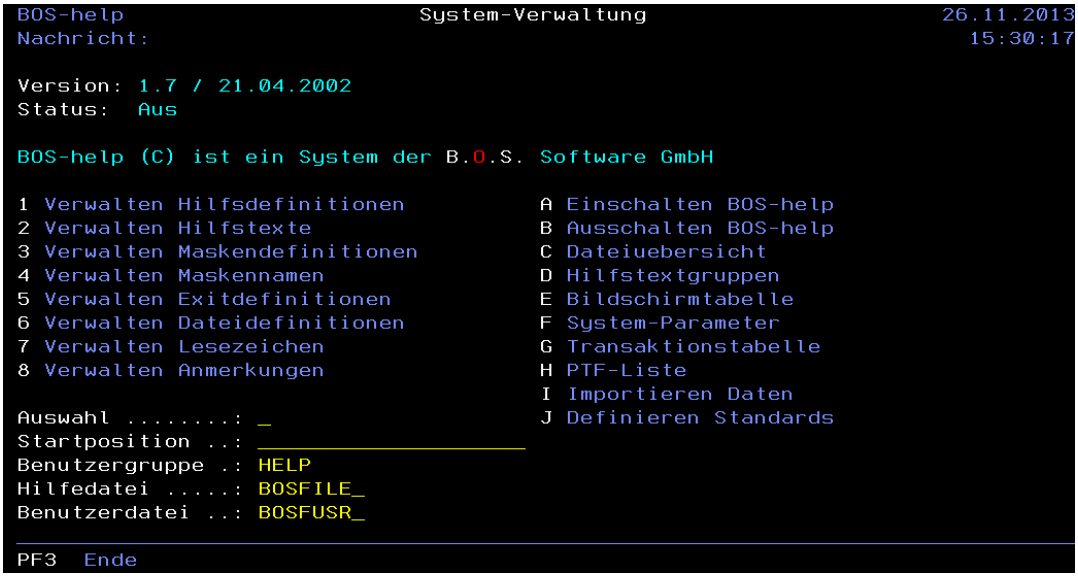
Mit dieser Option kann entschieden werden, ob ein Screenshot schwarz/weiß oder farbig gedruckt werden soll, oder ob er als Grafik in die Zwischenablage kopiert werden soll. Abhängig von der getroffenen Auswahl stehen weiter Optionen zur Verfügung.

Ausrichtung

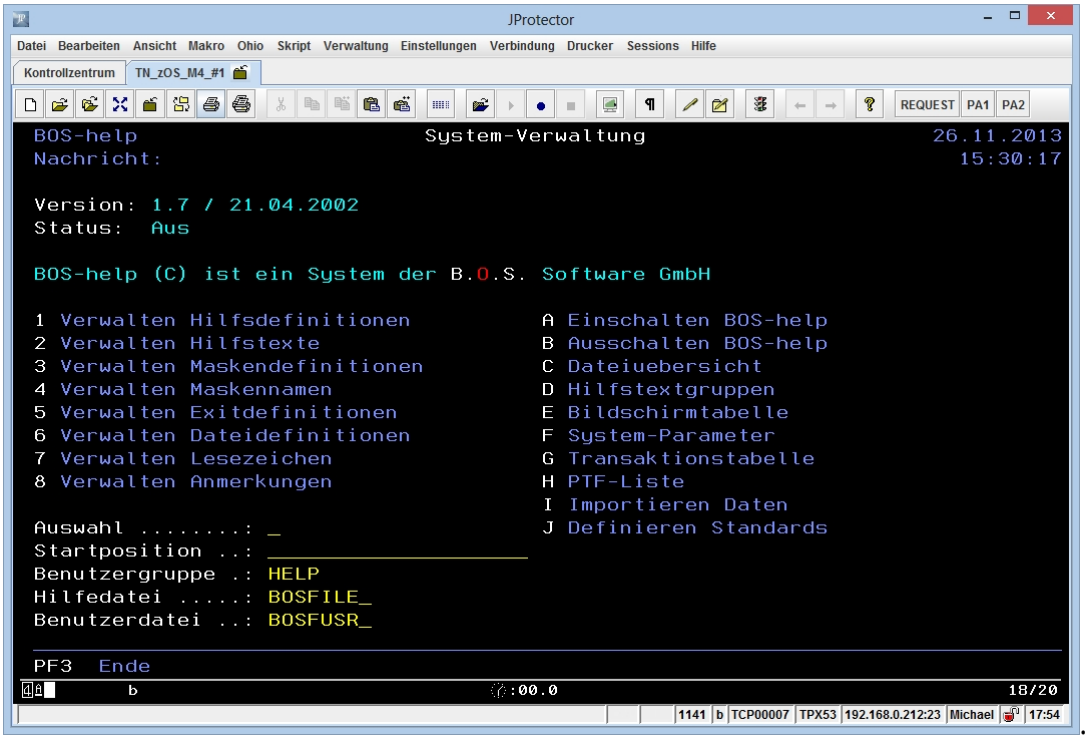
Wenn ein Screenshot auf einen Drucker ausgegeben werden soll (Typen schwarz/weiß, farbig) ist hier festzulegen, ob der Ausdruck im Hochformat (Portrait) oder im Querformat (Landscape) erstellt werden soll.

Bereich

Wenn der Screenshot als Grafik in die Zwischenablage kopiert werden soll, kann entschieden werden, ob die Grafik lediglich der Emulationsbereich



oder das ganze JProtector Fenster enthalten soll



Ausgabe

Wenn ein Screenshot auf einen Drucker ausgegeben werden soll (Typen schwarz/weiß, farbig), kann der Anwender durch Anklicken des Buttons 'Drucker wählen' den Druckerauswahl Dialog einblenden und einen anderen als den momentan zugeordneten Drucker für den Ausdruck des Screenshots auswählen. Die hier getroffene Auswahl ist nur temporär und wird nicht gespeichert.

Kapitel

9

Telnet SSL/TLS

SSL/TLS ist ein standardisiertes Protokoll zur Sicherung von Daten, die über öffentliche Netze ausgetauscht werden. Sichere Internetprotokolle wie z. B. HTTPS basieren auf SSL/TLS.

Die Grundlage des SSL/TLS Protokolls bildet die Verschlüsselung der übertragenen Informationen sowie die optionale Authentisierung der Kommunikationspartner durch den Austausch von Zertifikaten. Im Rahmen des Verbindungsaufbaus wird ein sessionspezifisches Token, ein symmetrischer Schlüssel, ausgetauscht.

Sollte der Verbindungsaufbau erfolgreich verlaufen sein, werden sämtliche Daten, die über diese Verbindung ausgetauscht werden, unter Verwendung des symmetrischen Schlüssels verschlüsselt und damit für Dritte unkenntlich gemacht.

Um SSL/TLS unter JProtector für die Sicherung einer Kommunikation mit einem IBM Mainframe über Telnet einsetzen zu können, ist dies im Rahmen der Sessiondefinition durch die Aktivierung des entsprechenden Auswählkästchens, wie nachfolgend gezeigt, bekannt zu geben.

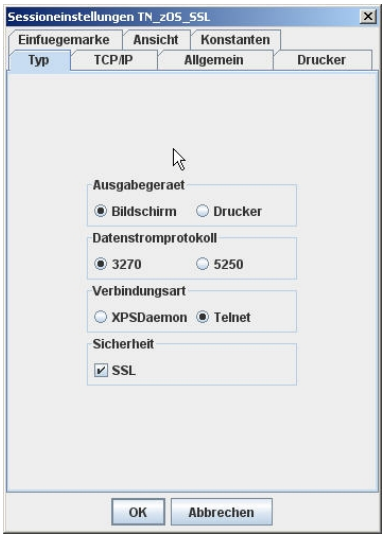


Abb. 39: Definition einer Telnet SSL/TLS Session

Weiterhin ist darauf zu achten, dass auf der Dialogseite 'TCP/IP' die erforderliche Portnummer korrekt eingestellt ist. Diese ist, falls sie nicht bekannt ist, bei einem zuständigen Mainframe-Administrator zu erfragen.

Falls weder Server- noch Clientauthentisierung gefordert werden, kann die Telnet SSL/TLS Session nach Abschluss dieser Definitionen unmittelbar gestartet werden. Andernfalls sind weitere Schritte, wie nachfolgend beschrieben, notwendig.

Diese Aussage ist allerdings nur richtig, falls eine Java VM größer oder gleich der Version 5 verwendet wird. Die Nutzung von Telnet SSL/TLS mit einer Java VM 1.4 erfordert die Verwendung eines Trusted Keystore wie weiter unten beschrieben.

Java Keystores

Eine Java Virtual Machine benutzt sogenannte 'Keystores' zur Speicherung und Verwaltung von privaten Schlüsseln und von digitalen X.509 Zertifikaten, die im Rahmen der Nutzung sicherheitsrelevanter Funktionen wie z. B. von SSL/TLS benötigt werden.

Die Verwaltung von Java Keystores erfolgt unter Verwendung von 'keytool.exe', einem Kommandozeilenprogramm, das Bestandteil der Java Laufzeitumgebung ist.

Nachfolgend wird davon ausgegangen, dass sowohl Client- als auch Serverauthentisierung verlangt werden. Daher ist es notwendig, dass die Java VM zur Laufzeit sowohl auf die benötigten Informationen zur Authentisierung des Clients als auch auf Informationen zur Gewährleistung der Integrität der vom verbundenen Server übermittelten Daten zugreifen kann. Dieser Umstand wird nachfolgend durch die Verwendung zweier Keystores berücksichtigt.

Client Keystore

Der Client Keystore dient zur Aufnahme des privaten Schlüssels sowie eines zugehörigen digitalen X.509 Zertifikats, das im Rahmen des SSL/TLS Handshake zur Authentisierung des Clients an den Server übermittelt wird.

Importieren der Informationen aus einer PKCS#12-Datei

Sollte der Client im Besitz einer PKCS#12 Datei sein, kann diese direkt in den Java Keystore für die Aufnahme der Clientinformationen importiert werden. Diese Funktion ist erst mit einem 'keytool' ab der Java Version 6 verfügbar.

Nachfolgend wird davon ausgegangen, dass der Aufruf von 'keytool' das entsprechende 'keytool.exe' startet, das sich im 'bin'-Verzeichnis der installierten Java Virtual Machine befindet. Eine Übersicht aller von 'keytool' unterstützten Parameter und Optionen kann durch Aufruf von 'keytool -help' angezeigt werden. Wie bereits erwähnt bieten verschiedene Versionen von 'keytool' einen unterschiedlichen Umfang an Funktionen an. Darüber hinaus kann die Parameterbezeichnung zwischen verschiedenen Versionen variieren.

Das Importieren der PKCS#12 Datei erfolgt beispielhaft mit dem folgenden Befehl:

```
keytool -importkeystore -destkeystore client.keystore -deststorepass secret
-destkeypass secret -destalias martina -srckeystore martina.p12
-srcstorepass secret -srcstoretype PKCS12 -alias 1
```

Parameter	Bedeutung
-importkeystore	Dieser Parameter weist 'keytool' an, Informationen aus einem vorhandenen Schlüsselspeicher zu importieren.
-destkeystore	Mit diesem Parameter wird der Keystore angegeben, in den 'keytool' die Informationen aus der PKCS#12 Datei importieren soll.
-deststorepass	Angabe des Passwortes für den Java Keystore, in den die Informationen aus der PKCS#12 Datei importiert werden sollen. Jeder Java Keystore ist mit einem Passwort geschützt. Das Passwort des Keystores muss zur Ausführung von 'keytool' Funktionen bekannt sein. Man kann das Passwort, wie im Beispiel gezeigt, als Parameter beim Aufruf von 'keytool' angeben. Wird dieser Parameter nicht angegeben, erfragt 'keytool' das Passwort vor Ausführung des Kommandos. In

	diesem Fall wird das eingegebene Passwort nicht durch ein Echo an der Konsole ausgegeben, so dass Dritte es nicht lesen können.
-destkeypass	Das Passwort, mit dem der importierte Schlüssel geschützt werden soll. Wenn diese Angabe fehlt, erfragt 'keytool' das Passwort. Ansonsten gilt das für '–dest-storepass' gesagte.
-destalias	Der Alias-Name dient im Rahmen nachfolgender Aufrufe von 'keytool' zur Identifizierung des importierten Schlüssels.
-srckeystore	Mit diesem Parameter wird der Name der PKCS#12 Datei angegeben, aus der 'keytool' die Informationen importieren soll.
-srcstorepass	Angabe des Passwortes, mit dem die PKCS#12 Datei verschlüsselt wurde.
-srcstoretype	Mit diesem Parameter erfolgt die Angabe des Typs des Schlüsselspeichers, aus dem 'keytool' die Informationen importieren soll. Im Falle einer PKCS#12 Datei ist hier die Angabe 'PKCS12' erforderlich.
-alias	Mit diesem Aliasnamen ist der gewünschte Schlüssel in der PKCS#12 Datei zu identifizieren. Hier ist immer der Wert '1' anzugeben.

Generieren eines privaten Schlüssels mit einem Zertifikatsrequest

Sollte keine private Schlüsselinformation in Form einer PKCS#12 Datei vorliegen und Clientauthentisierung erforderlich sein, besteht die Möglichkeit, diese unter Verwendung von 'keytool' zu erstellen.

Dazu ist zunächst ein privater Schlüssel zu generieren. Unter Verwendung des generierten Schlüssels wird anschließend ein Zertifikatsantrag erstellt, der dann an die CA (Certificate Authority) des Hosts, mit dem eine SSL/TLS Telnetverbindung aufgebaut werden soll, zu übermitteln ist.

Die Host CA erstellt aus diesem Zertifikatsantrag ein Zertifikat für die Anwenderin, das anschließend, zusammen mit allen eventuell benötigten Ausstellerzertifikaten, in den Java Client Keystore zu importieren ist.

Generierung eines privaten Schlüssels

Die Generierung eines privaten Schlüssels erfolgt beispielhaft mit dem folgenden Befehl:

```
keytool -genkey -dname "cn=Martina Musterfrau, ou=Einkauf, o=Muster GmbH, c=DE"
-alias muster -keystore client.keystore -storepass secret –keypass secret
```

Da für den Keystore keine Pfadangabe erfolgt, wird der Keystore aus dem aktuellen Verzeichnis verwendet. Sollte der Keystore nicht existieren, wird er durch die Ausführung dieses Befehls erstellt.

Parameter	**Bedeutung**
-genkey	Dieser Parameter weist 'keytool' an, einen privaten Schlüssel zu generieren.
-dname	Mit diesem Parameter können spezifische Angaben für die Anwenderin gemacht werden, für die der Schlüssel erstellt wird.
-alias	Der Alias-Name dient im Rahmen nachfolgender Aufrufe von 'keytool' zur Identifizierung des Schlüssels.
-keystore	Mit diesem Parameter wird der Keystore angegeben, auf dem 'keytool' operieren soll.
-storepass	Jeder Java Keystore ist mit einem Passwort geschützt. Das Passwort des Keystores muss zur Ausführung von 'keytool' Funktionen bekannt sein. Man kann das Passwort, wie im Beispiel gezeigt, als Parameter beim Aufruf von 'keytool' angeben. Wird dieser Parameter nicht angegegen, erfragt 'keytool' das Passwort vor Ausführung des Kommandos. In diesem Fall wird das eingegebene Passwort nicht durch ein Echo an der Konsole ausgegeben, so dass Dritte es nicht lesen können.

-keypass	Das Passwort, mit dem der erstellte Schlüssel geschützt werden soll. Wenn diese Angabe fehlt, erfragt 'keytool' das Passwort. Ansonsten gilt das für '–storepass' gesagte.

Der Inhalt des Keystore kann durch Aufruf des folgenden Kommandos angezeigt werden:

```
keytool -list -keystore client.keystore -storepass secret
```

Nachfolgend ist eine mögliche Ausgabe aufgelistet:

```
Keystore-Typ: JKS
Keystore-Provider: SUN

Ihr Keystore enthält 1 Eintrag/-äge.

muster, 06.03.2007, PrivateKeyEntry,
Zertifikatsfingerabdruck (MD5): 81:81:BE:43:1A:13:97:93:CB:BA:29:02:C5:0A:2C:5F
```

Erstellung eines Zertifikatsantrags

Mit dem folgenden Befehl ist nun unter Verwendung des generierten privaten Schlüssels ein Zertifikatsantrag zu erstellen.

```
keytool -certreq -alias muster -keystore client.keystore -storepass secret -file
muster.csr
```

Parameter	Bedeutung
-certreq	Dieser Parameter weist 'keytool' an, einen Zertifikatsantrag zu generieren.
-alias	Mit Alias-Name wird der private Schlüssel identifiziert, für den der Zertifikatsantrag erstellt werden soll.
-keystore	Mit diesem Parameter wird der Keystore angegeben, auf dem 'keytool' operieren soll.
-storepass	Hier ist das Passwort anzugeben, mit dem der Keystore geschützt wurde. Wenn diese Angabe entfällt, erfragt 'keytool' das Passwort von der Anwenderin.
-file	Mit diesem Parameter ist der Name der Datei anzugeben, die den generierten Zertifikatsantrag aufnehmen soll.

Nach Ausführung des Befehls befindet sich im aktuellen Verzeichnis eine Datei namens 'muster.csr', die den Zertifikatsantrag enthält.

Diese Datei ist an die entsprechende CA (Certification Authority) zu übermitteln. Unter IBM z/OS kann z. B. RACF (Resource Access Control Facility) als CA fungieren.

Unter Verwendung des Zertifikatsantrags erstellt die CA ein Zertifikat für die Anwenderin und stellt dieses für die weitere Verarbeitung zur Verfügung. Darüber hinaus muss die CA der Anwenderin sämtliche Ausstellerzertifikate, die zur Generierung des Zertifikats herangezogen wurden, zur Verfügung stellen.

Importieren der Ausstellerzertifikate sowie des Zertifikats für die Anwenderin

Vor dem Importieren des Zertifikates, das die CA für die Anwenderin erstellt und in der Datei 'muster.cer' bereitgestellt hat, muss die gesamte Kette der Ausstellerzertifikate in den Keystore importiert werden. In unserem Beispiel gibt es genau ein Ausstellerzertifikat, das die CA unter dem Namen 'xpsca.cer' bereitgestellt hat. Das Ausstellerzertifikat (Trusted Signer) ist mit dem nachfolgenden Befehl in den Client Keystore zu importieren:

```
keytool -import –alias xpsca -keystore client.keystore -storepass secret -file
xpsca.cer
```

Als Antwort listet 'keytool' einige Informationen über das Ausstellerzertifikat auf und bittet die Anwenderin die Vertrauenswürdigkeit des Ausstellerzertifikats durch Eingabe von 'ja' zu bestätigen. Nach erfolgter Bestätigung importiert 'keytool' das Zertifikat in den Keystore.

Parameter	Bedeutung
-import	Dieser Parameter weist 'keytool' an, ein Zertifikat zu importieren.
-alias	Mit der Angabe für den Alias-Namen wird festgelegt, unter welchem Namen das zu importierende Zertifikat nachfolgend identifiziert werden soll.
-keystore	Mit diesem Parameter wird der Keystore angegeben, in den das Zertifikat importiert werden soll.
-storepass	Hier ist das Passwort anzugeben, mit dem der Keystore geschützt wurde. Wenn diese Angabe entfällt, erfragt 'keytool' das Passwort von der Anwenderin.
-file	Mit diesem Parameter ist der Name der Datei anzugeben, die das zu importierende Zertifikat enthält.

Nachdem alle benötigten Ausstellerzertifikate importiert wurden ist schließlich noch das Zertifikat der Anwenderin zu importieren.

```
keytool -import –alias muster -keystore client.keystore -storepass secret -file
muster.cer
```

Die Parameter dieses Import Befehls entsprechen den zuvor beschriebenen. Es ist jedoch zu beachten, dass der verwendete Alias-Name dem Namen entspricht, der bei der Generierung des privaten Schlüssels für die Anwenderin vergeben wurde.

Durch erneute Ausführung des List-Befehls kann der aktuelle Inhalt des Keystore angezeigt werden:

```
keytool -list -keystore client.keystore -storepass secret
```

Nachfolgend ist eine mögliche Ausgabe aufgelistet:

```
Keystore-Typ: JKS
Keystore-Provider: SUN

Ihr Keystore enthält 2 Einträge.

xpsca, 06.03.2007, trustedCertEntry,
Zertifikatsfingerabdruck (MD5): EC:BC:4B:F5:6D:0E:E6:C0:F2:5C:AF:CD:29:0C:33:04
muster, 06.03.2007, PrivateKeyEntry,
Zertifikatsfingerabdruck (MD5): C1:67:48:71:87:67:A9:DF:08:B5:92:B4:BA:7B:A2:7B
```

Trusted Keystore

Ein Trusted Keystore dient zur Aufnahme von Zertifikaten vertrauenswürdiger Aussteller. Im Rahmen des SSL/TLS Verbindungsaufbaus übermittelt der Server ein Zertifikat zur Authentisierung. Damit dieses Zertifikat clientseitig akzeptiert wird, muss sich das Ausstellerzertifikat des Serverzertifikats im Trusted Keystore befinden.

Das Ausstellerzertifikat des Serverzertifikats ist bei der entsprechenden Stelle zu beziehen, bei der Telnet SSL/TLS verwaltet wird.

Importieren des vertrauenswürdigen Ausstellerzertifikats

In unserem Beispiel wurde das Ausstellerzertifikat des Serverzertifikats als 'xpsca.cer' zur Verfügung gestellt. Dieses Zertifikat ist nun in einen Keystore zu importieren, der vertrauenswürdige Ausstellerzertifikate speichert.

Das Ausstellerzertifikat (Trusted Signer) ist mit dem nachfolgenden Befehl in den Client Keystore zu importieren:

```
keytool -import –alias xpsca -keystore trusted.keystore -storepass secret -file
xpsca.cer
```

Als Antwort listet 'keytool' einige Informationen über das Ausstellerzertifikat auf und bittet die Anwenderin die Vertrauenswürdigkeit des Ausstellerzertifikats durch Eingabe von 'ja' zu bestätigen. Nach erfolgter Bestätigung importiert 'keytool' das Zertifikat in den Keystore.

Parameter	Bedeutung
-import	Dieser Parameter weist 'keytool' an, ein Zertifikat zu importieren.
-alias	Mit der Angabe für den Alias-Namen wird festgelegt, unter welchem Namen das zu importierende Ausstellerzertifikat nachfolgend identifiziert werden soll.
-keystore	Mit diesem Parameter wird der Keystore angegeben, in den das Ausstellerzertifikat importiert werden soll. Sollte der Keystore nicht existieren wird er durch die Ausführung des Imports erstellt.
-storepass	Hier ist das Passwort anzugeben, mit dem der Keystore geschützt ist. Wenn diese Angabe entfällt, erfragt 'keytool' das Passwort von der Anwenderin.
-file	Mit diesem Parameter ist der Name der Datei anzugeben, die das zu importierende Ausstellerzertifikat enthält.

Durch Ausführung des List-Befehls kann der aktuelle Inhalt des Keystore angezeigt werden:

```
keytool -list -keystore trusted.keystore -storepass secret
```

Nachfolgend ist eine mögliche Ausgabe aufgelistet:

```
Keystore-Typ: JKS
Keystore-Provider: SUN

Ihr Keystore enthält 1 Eintrag/-äge.

xpsca, 06.03.2007, trustedCertEntry,
Zertifikatsfingerabdruck (MD5): EC:BC:4B:F5:6D:0E:E6:C0:F2:5C:AF:CD:29:0C:33:04
```

Mit der Fertigstellung des Trusted Keystore stehen clientseitig alle benötigten Daten für die Nutzung von SSL/TLS Telnet zur Verfügung und die erstellten Keystores können je nach Bedarf im Rahmen der allgemeinen Verwaltung von JProtector wie im Kapitel 'Allgemeine Einstellungen – Telnet Sicherheit' auf Seite '39' beschrieben, bekannt gegeben werden.

Kapitel

10

Digitale Zertifikate

Digitale Zertifikate zur Benutzerauthentisierung erlangen zunehmend größere Bedeutung, z. B. durch den Einsatz im Rahmen der Installation einer PKI (Public Key Infrastructure). Das Applikationssystem JProtector/XPSDaemon unterstützt die Verwendung von digitalen X.509 Zertifikaten in der Version 3.

Dies bietet einem Benutzer einerseits die Möglichkeit, sich gegenüber XPSDaemon durch ein digitales Zertifikat zu authentisieren. Wenn XPSDaemon ein Zertifikat als gültig akzeptieren soll, muss das zugehörige Ausstellerzertifikat als vertrauenswürdig angesehen werden. Dazu ist das Ausstellerzertifikat in XPSDaemon zu importieren.

Andererseits kann benutzerseitig gefordert werden, dass sich das XPSDaemon Hostsystem, mit dem eine Verbindung aufgebaut werden soll, durch ein X.509 Zertifikat authentisiert. Damit kann ein Anwender sicherstellen, mit einem bestimmten Hostrechner zu kommunizieren. In diesem Fall ist zu berücksichtigen, dass bei aktivierter Serverauthentisierung hostseitig ein RSA Entschlüsselungsvorgang durchgeführt werden muss. Dies kann zu merklicher Performanceeinbuße beim Verbindungsaufbau führen.

Im Rahmen der XPSDaemon Profileverwaltung kann verlangt werden, eine Anmeldung an das Hostsystem nur unter Verwendung eines X.509 Zertifikates, das von einem als vertrauenswürdig gekennzeichneten Aussteller herausgegeben wurde, zuzulassen. Auf diese Weise kann eine effektive Zugangsbeschränkung installiert werden.

Zur Erzielung größtmöglicher Sicherheit verzichtet JProtector auf jegliche Speicherung von Passwörtern, mit Hilfe derer PKCS#12 Dateien, die Benutzerzertifikate und private Schlüssel enthalten, verschlüsselt wurden. Daher erfragt JProtector bei jedem Aufbau einer Session, die ein Zertifikat zur Authentisierung einsetzt, das Passwort, mit dem der Inhalt der PKCS#12 Datei verschlüsselt wurde.

Benutzerauthentisierung

Zertifikate, die zur Benutzerauthentisierung verwendet werden sollen, sind zunächst in die JProtector Datenbasis zu importieren. Dazu steht der Menüpunkt 'Verwaltung::Zertifikate' bereit. Die Verwaltung der PKCS#12 Dateien erfolgt über den nachfolgend abgebildeten Dialog.

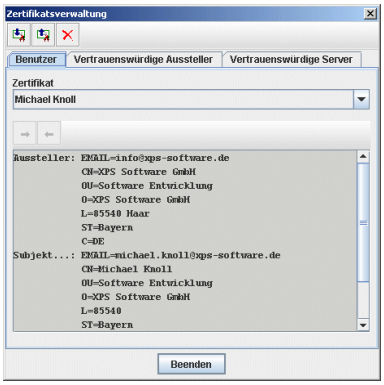


Abb. 40: Verwaltung von Benutzerzertifikaten

Der Dialog stellt die folgenden Funktionen zur Zertifikatsverwaltung bereit:

, Nächstes in Kette/Vorheriges in Kette

Sollte die ausgewählte PKCS#12 Datei mehr als ein Zertifikat enthalten, kann mit diesen Schaltflächen zwischen den verschiedenen Zertifikaten geblättert werden. Wenn eine PKCS#12 Datei mehrere Zertifikate enthält, befinden sich darin neben dem Benutzerzertifikat auch noch ein oder mehrere Ausstellerzertifikate.

Importieren

Mit dieser Funktion können neue Zertifikate in die JProtector Datenbasis importiert werden. Dazu wird ein Dateiauswahldialog eingeblendet, in dem der Speicherort der PKCS#12 Datei auszuwählen ist, die importiert werden soll.

Nach der Auswahl der Datei erfragt JProtector das Passwort, das zur Verschlüsselung der Daten in der PKCS#12 Datei verwendet wurde. Nach dem Importieren steht das Zertifikat zur Verwendung in Sessions zur Verfügung.

Hinweis: JProtector kann PKCS#12 Dateien importieren, die von den neueren Browserversionen von Microsoft (*.pfx) und Netscape (*.p12) exportiert werden.

Exportieren

Zuvor importierte PKCS#12 Dateien können unter Verwendung dieser Funktion wieder exportiert werden. Die exportierte Datei ist eine 1:1 Kopie der zuvor importierten PKCS#12 Datei.

Löschen

Mit dieser Funktion können Zertifikate, die nicht verwendet werden, aus der JProtector Datenbasis gelöscht werden.

Serverauthentisierung

Es folgt eine kurze Beschreibung der Schritte, die von JProtector durchgeführt werden, falls Serverauthentisierung für eine Session verlangt wird. Die Vorgehensweise zur Aktivierung der Serverauthentisierung ist in Kapitel 'Sessioneinstellungen - Sicherheit' auf Seite 52 beschrieben.

Zunächst teilt JProtector XPSDaemon im Rahmen des Sessionaufbaus mit, dass Serverauthentisierung verlangt wird.

Sollte XPSDaemon nicht dazu in der Lage sein, ein X.509 Zertifikat an JProtector zu übermitteln, wird der Verbindungsaufbau von JProtector abgebrochen.

Andernfalls wird überprüft, ob die JProtector Datenbasis ein Zertifikat enthält, das den Aussteller des Serverzertifikates als vertrauenswürdig ausweist. Zertifikate von Ausstellern, die als vertrauenswürdig angesehen werden sollen, können im Rahmen der Zertifikatsverwaltung in die JProtector Datenbasis geladen werden. Dies erfolgt mit Hilfe der folgenden Dialogseite:

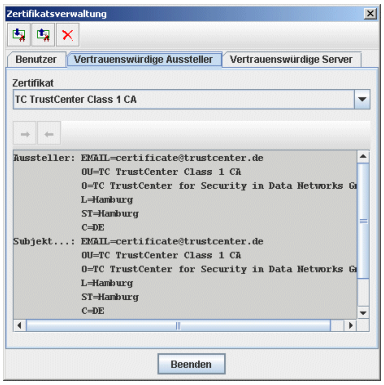


Abb. 41: Verwaltung von Ausstellerzertifikaten

Importieren

Mit dieser Funktion können neue Ausstellerzertifikate in die JProtector Datenbasis importiert werden. Dazu wird ein Dateiauswahldialog eingeblendet, in dem der Speicherort der Zertifikatsdatei auszuwählen ist, die importiert werden soll.

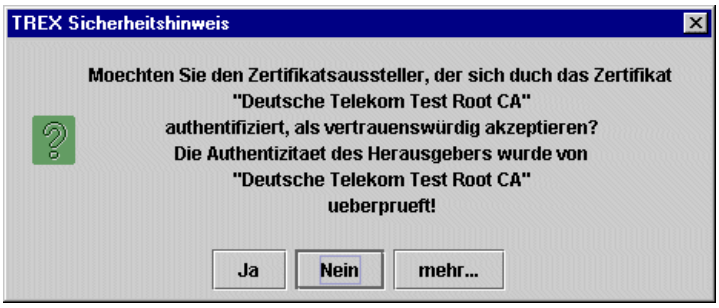
Exportieren

Zuvor importierte Zertifikatsdateien können unter Verwendung dieser Funktion wieder exportiert werden. Die exportierte Datei ist eine 1:1 Kopie der zuvor importierten Datei.

Löschen

Mit dieser Funktion können Zertifikate von Ausstellern, die nicht länger als vertrauenswürdig angesehen werden sollen, aus der JProtector Datenbasis gelöscht werden.

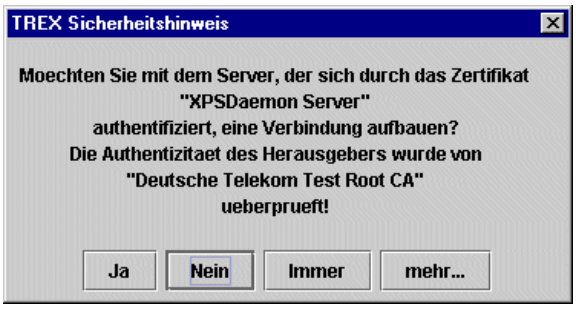
XPSDaemon kann bei Bedarf zusammen mit dem Serverzertifikat auch das verwendete Ausstellerzertifikat an JProtector übermitteln. Sollte diese Variante gewählt werden, ist das vorherige Importieren des Ausstellerzertifikats in die JProtector Datenbasis nicht notwendig. In diesem Fall blendet JProtector den folgenden Dialog ein:



Der Benutzer muss nun durch Auswahl einer der möglichen Schaltflächen entscheiden, ob er den Aussteller für vertrauenswürdig erachtet. Nach Auswahl der Schaltfläche 'mehr...' werden nähere Informationen über das Ausstellerzertifikat eingeblendet.

Falls 'Nein' gewählt wird, bricht JProtector den Verbindungsaufbau ab. Bei 'Ja' importiert JProtector das übermittelte Ausstellerzertifikat in die Datenbasis und dieser Aussteller wird daraufhin als vertrauenswürdig angesehen.

Nach der Auswahl von 'Ja' blendet JProtector den folgenden Dialog ein, der Informationen über das erhaltene Serverzertifikat enthält.



Bei Auswahl der Schaltfläche 'mehr' werden weitere Informationen zum Zertifikat angezeigt. 'Nein' führt zum Abbruch des Verbindungsaufbaus durch JProtector. Die Wahlmöglichkeiten 'Ja' und 'Immer' haben zur Folge, dass der Verbindungsaufbau fortgesetzt wird.

Der Unterschied besteht darin, dass JProtector das übermittelte Serverzertifikat bei Auswahl von 'Immer' in die Datenbasis importiert. Das bedeutet, dass Server, die sich bei zukünftigen Verbindungsaufbauten mit diesem Zertifikat authentisieren, automatisch als vertrauenswürdig angesehen werden.

Falls 'Ja' ausgewählt wird, erfolgt kein Import des Serverzertifikates. Damit wird der oben abgebildete Dialog beim nächsten Verbindungsaufbau erneut angezeigt.

Die Verwaltung der geladenen Serverzertifikate erfolgt mit der folgenden Dialogseite:

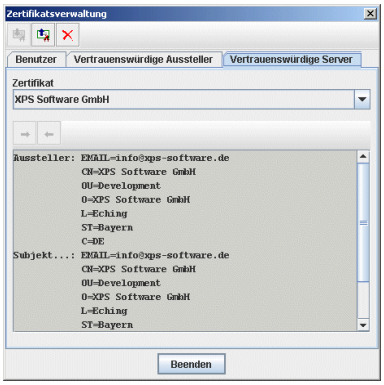


Abb. 42: Verwaltung von Serverzertifikaten

Exportieren

Zertifikate von vertrauenswürdigen Servern können unter Verwendung dieser Funktion exportiert werden.

Löschen

Mit dieser Funktion können Zertifikate von Servern, die nicht länger als vertrauenswürdig angesehen werden sollen, aus der JProtector Datenbasis gelöscht werden.

Hinweis: Die beschriebene Vorgehensweise zur Serverauthentisierung ist im Allgemeinen nur einmal durchzuführen. Falls sich Aussteller- und Serverzertifikat in der JProtector Datenbasis befinden, erfolgt die Serverauthentisierung automatisch im Hintergrund.

Kapitel

11

Makros

Bei der Arbeit in einer Großrechnerumgebung fallen eine Reihe von Aufgaben an, die regelmäßig oder zumindest häufiger auszuführen sind.

Normalerweise handelt es sich hierbei um eine Abfolge von Tastatureingaben. Die Bearbeitung mehrerer Masken bis zum Erreichen eines gewünschten Bildschirms oder die Ausführung syntaktisch komplizierter Systembefehle sind nur einige Beispiele.

Zur Vereinfachung der Ausführung von sich wiederholenden Tastatureingabefolgen ermöglicht JProtector die Aufzeichnung von Makros.

Dazu ist eine Abfolge von Tastatureingaben einmal exemplarisch aufzuzeichnen und unter einem eindeutigen Namen in der JProtector Datenbasis abzuspeichern.

Zu einem späteren Zeitpunkt kann das aufgezeichnete Makro dann durch Ausführung eines einfachen Befehls oder durch Drücken einer zugewiesenen Tastenkombination ausgeführt werden, ohne dass der Benutzer die Eingaben wiederholt durchführen muss.

Es folgt eine Beschreibung der einzelnen Schritte von der Aufzeichnung eines Makros bis zu seiner Ausführung.

Aufzeichnung eines Makros

Zur Vorbereitung der Aufzeichnung eines Makros ist zunächst sicherzustellen, dass der Startbildschirm für die Aufzeichnung im JProtector Emulationsfenster angezeigt wird.

Daraufhin ist mit der Aufzeichnung des Makros zu beginnen. Dies kann auf verschiedene Arten bewerkstelligt werden.

Entweder geschieht dies durch Auswahl des Menüpunktes 'Makro::Aufzeichnen' bzw. durch Drücken einer, der Funktion zugewiesenen, Taste(nkombination), oder durch Auswahl der Schaltfläche in der Befehlsleiste der JProtector Arbeitsoberfläche.

Daraufhin zeichnet JProtector alle Tastatureingaben und Markiervorgänge mit der Maus auf.

Zunächst ist es dabei empfehlenswert, die Einfügemarke durch eine definierte Tastenkombination an der Position der ersten Zeicheneingabe zu platzieren. Das kann z. B. durch Drücken der Pos1 Taste und anschließendes Verschieben der Einfügemarke mittels der Tabulatortaste oder den Richtungstasten geschehen.

Nachdem alle aufzuzeichnenden Tastatureingaben gemacht worden sind, ist der Aufzeichnungsvorgang durch Auswahl des Menüpunktes 'Makro::Stoppen' oder einer, der Funktion zugewiesenen, Taste(nkombination) zu beenden. Alternativ kann die Schaltfläche ■ in der Befehlsleiste durch Mausklick gedrückt werden.

Daraufhin blendet JProtector den nachfolgend abgebildeten Dialog zum Speichern des aufgezeichneten Makros in der JProtector Datenbasis ein:

Abb. 43: Makro speichern unter

Zur Erleichterung der Gruppierung von Makros können Unterverzeichnisse zum Verzeichnis 'Macros' auf der JProtector Datenbasis erstellt werden. Dazu ist das Oberverzeichnis im abgebildeten Dialog zu markieren und ein Verzeichnis zu erstellen.

Dies geschieht durch Drücken der Schaltfläche 'Verzeichnis erstellen'. Daraufhin wird ein Dialog eingeblendet, in dem der Name für das zu erstellende Verzeichnis einzugeben ist.

Zum Speichern des aufgezeichneten Makros ist zunächst das Verzeichnis im abgebildeten Dialog zu markieren, in dem das Makro gespeichert werden soll. Danach ist der Makroname im Eingabefeld 'Dateiname' zu vergeben und die Schaltfläche 'OK' zu drücken.

Hinweis: Innerhalb eines Verzeichnisses müssen sowohl die Namen der einzelnen Unterverzeichnisse, als auch die der Makros eindeutig sein. Bei Verletzung dieser Regel erlaubt JProtector das Speichern eines Makros oder die Erstellung eines Unterverzeichnisses nicht. Außerdem darf ein Verzeichnisname nicht das Pfadtrennzeichen '/' enthalten.

Mit der Speicherung des Makros ist der Aufzeichnungsvorgang beendet und das Makro steht zur späteren Ausführung zur Verfügung.

Abspielen eines Makros

Zum Abspielen eines Makros gibt es verschiedene Möglichkeiten.

Für häufig benötigte Makros empfiehlt sich die Zuweisung der Makroausführung an eine Tastenkombination. Die Vorgehensweise hierzu ist im Kapitel 'Tastenzuweisung – Makros' auf Seite 80 beschrieben.

Nach erfolgter Tastenzuweisung kann das Makro einfach durch Drücken der zugewiesenen Tastenkombination ausgeführt werden.

Wenn die Ausführung von Makros häufig in Anspruch genommen wird, ist zu erwägen, ob das Einblenden des Makropads im linken Bereich der JProtector Arbeitsoberfläche sinnvoll ist, was durch Auswahl des Menüpunktes 'Anzeige::Makropad' erfolgen kann.

Das Makropad enthält eine Baumdarstellung aller aufgezeichneten Makros. Bei eingeblendetem Pad kann die Ausführung des Makros durch Doppelklick mit der Maus auf den Makronamen gestartet werden.

Eine weitere Möglichkeit zum Abspielen von Makros bieten spezielle Menüfunktionen.

Bei Verwendung des Menüpunktes 'Makro::Laden' wird ein Dateiauswahldialog eingeblendet, mit dessen Hilfe das zu ladende Makro auszuwählen ist. Nach erfolgter Auswahl wird das Makro sofort abgespielt.

Das aktive Makro kann auch durch Auswahl der Menüpunktes 'Makro::Abspielen' oder durch Klicken der Schaltfläche in der JProtector Befehlsleiste erneut ausgeführt werden.

Der Makroverwaltungsdialog

JProtector stellt zur Verwaltung von Makros den nachfolgend abgebildeten Dialog zur Verfügung. Der Dialog kann durch Auswahl des Menüpunktes 'Verwaltung::Makros' eingeblendet werden.

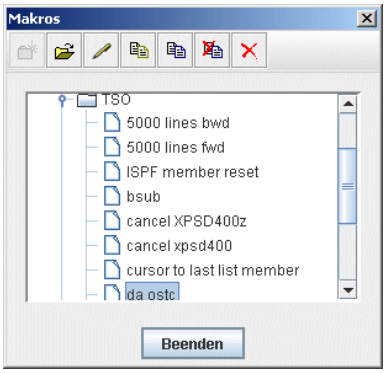


Abb. 44: Makroverwaltung

Verzeichnis erstellen

Unter Verwendung dieser Schaltfläche kann ein neues Unterverzeichnis erstellt werden. Die Verwendung von Verzeichnissen erleichtert die Gruppierung verwandter Makros.

Zur Erstellung eines Verzeichnisses ist zunächst das Verzeichnis im Baum zu markieren, unter dem das neue Verzeichnis erstellt werden soll und dann die Schaltfläche anzuklicken. Der Name für das Verzeichnis ist im daraufhin eingeblendeten Dialog einzugeben.

Unterverzeichnisnamen innerhalb eines Verzeichnisses müssen eindeutig sein.

Laden

Wenn diese Schaltfläche bei markiertem Makronamen gedrückt wird, wird das gewählte Makro von JProtector geladen und ausgeführt.

Bearbeiten

JProtector ermöglicht das nachträgliche Bearbeiten von Makros. Dazu ist bei ausgewähltem Makro diese Schaltfläche zu drücken. Die Beschreibung des JProtector Makroeditors erfolgt im nächsten Abschnitt.

Umbenennen

Zum Umbenennen eines Makros ist dar Makroname zunächst im Baum zu markieren und dann diese Schaltfläche anzuklicken. Daraufhin wird ein Dialog eingeblendet, in dem der neue Name für das Makro eingegeben werden kann.

Die Namen aller Makros innerhalb eines Verzeichnisses müssen eindeutig sein.

Kopieren

Makros können innerhalb des Makroverzeichnisbaums kopiert werden.

Der Kopiervorgang verläuft identisch zum Verschiebevorgang mit dem Unterschied, dass das gewählte Makro in seinem ursprünglichen Verzeichnis erhalten bleibt.

Verschieben

Ein Makro kann innerhalb des Makroverzeichnisbaumes verschoben werden. Dazu ist zunächst der Makroname zu markieren und anschließend die Schaltfläche 'Verschieben' anzuklicken.

Daraufhin wird der weiter oben beschriebene Dialog zum Speichern eines Makros eingeblendet, in dem das Zielverzeichnis für die Verschiebeoperation auszuwählen ist.

Wenn gewünscht, kann das Makro im Rahmen der Verschiebung umbenannt werden. Es gilt auch hier die Regel, dass der Makroname im Zielverzeichnis eindeutig sein muss.

Löschen

Das Löschen eines Makros erfolgt durch Markieren des Makros und anschließendem Klicken auf die Schaltfläche 'Löschen'.

Hinweis: Bei der Ausführung von Makroverwaltungsfunktionen überprüft JProtector, ob sich Veränderungen auf bereits durchgeführte Tastenzuweisungen auswirken. Sollte z. B. ein Makro gelöscht werden, wird implizit eine eventuell vorhandene Zuweisung der Makroausführung an eine Tastenkombination entfernt.

Der Makroeditor

Unter Verwendung des JProtector Makroeditors kann ein Anwender nachträglich Veränderungen an aufgezeichneten Makros vornehmen.

Dazu ist das Makro zunächst im Makro Verwaltungsdialog zu markieren und anschließend die Schaltfläche für 'Bearbeiten' zu drücken. Daraufhin wird ein Dialog eingeblendet, der die einzelnen Makroschritte auflistet:

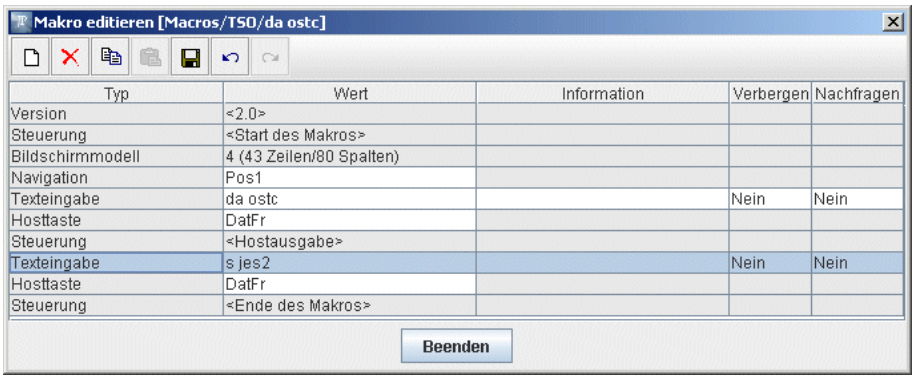


Abb. 45: Makroeditor

Das gezeigte Makro ruft in einer TSO/SDSF Session die Anzeige der momentan aktiven Started Tasks auf ('da ostc') und beschränkt anschließend die Anzeige auf die JES2 Region ('s jes2'). Zur Ausübung der jeweiligen Befehle wird die Datenfreigabetaste ausgelöst.

Beschreibung der Dialogfelder

Jeder Makroschritt ist in einer separaten Tabellenzeile aufgelistet. Für manche Makroschritte ist eine Auswahl an Informationen editierbar. Diese Informationen befinden sich in Weiß hinterlegten Feldern. Alle anderen Informationen sind nicht editierbar.

In der ersten Spalte ('Typ') befindet sich eine Beschreibung des Makroschritts. JProtector fügt zu Beginn der Aufzeichnung eines Makros einige Schritte ein, die interne Informationen wie z. B. die Version des Makroeditors enthalten.

In der zweiten Spalte ('Wert') werden die relevanten Daten für jeden Makroschritt angezeigt. Die Art der gezeigten Information ist vom Typ des Makroschritts abhängig. Insbesondere werden hier Navigations- und Hosttasten sowie Texteingaben angezeigt.

Die dritte Spalte ('Information') zeigt zusätzliche Informationen an, die für ausgewählte Makroschritte gespeichert werden können. Hierbei handelt es sich um Kommentare, die für den Anwender bei der späteren Analyse des Makros hilfreich sein können.

In der vierten Spalte ('Verbergen') kann festgelegt werden, ob die in Spalte 2 ('Wert') gespeicherte Information sichtbar sein soll oder nicht. Bei der Aufzeichnung von Informationen, die in Dunkelfelder eingegeben werden, setzt JProtector dieses Attribut automatisch auf 'Ja'.

Unter Verwendung der fünften Spalte ('Nachfragen') kann der Anwender festlegen, ob Texteingaben direkt so, wie aufgezeichnet, wiedergegeben werden sollen, oder ob JProtector beim Anwender einen aktuellen Wert erfragen soll.

Beschreibung der Editoren

Damit der Inhalt eines Feldes editiert werden kann, ist im entsprechenden Feld ein Doppelklick mit der Maus durchzuführen. Daraufhin wechselt das Feld in den Editormodus.

Bei Text- oder Zahleneingaben kann der gewünschte Wert direkt im Feld eingegeben werden. Alle anderen Informationen, die aus einer vordefinierten Wertemenge stammen müssen wie z. B. eine Hosttaste oder ein Entscheidungswert, können durch Auswahl des gewünschten Wertes aus einer Combobox aktiviert werden.

Toolbarfunktionen

Die Toolbar des Makroeditors bietet dem Anwender während der Bearbeitung leichten Zugriff auf eine Reihe nützlicher Funktionen. Einige Funktionen der Toolbar können nur ausgewählt werden, wenn einer oder mehrere Makroschritte markiert sind. Dieselben Funktionen können auch über ein Kontextmenü ausgewählt werden, das durch drücken der rechten Maustaste eingeblendet wird.

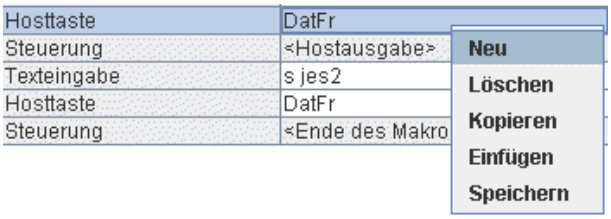


Abb. 46: Kontextmenü im Editor

Neu

Unter Verwendung dieser Schaltfläche kann ein neuer Makroschritt eingefügt werden. Dazu wird der folgende Dialog zur Auswahl des gewünschten Schritttyps angezeigt:

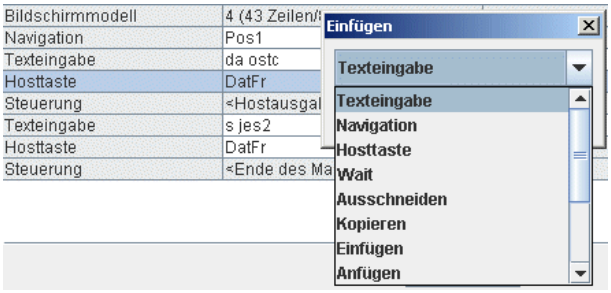


Abb. 47: Einfügen eines neuen Makroschritts

Der gewünschte Makroschritt ist in der Combobox zu markieren und die Auswahl ist durch Drücken der 'OK' Schaltfläche zu bestätigen. Daraufhin wird der folgende Dialog eingeblendet, mit dem die Position für den neuen Makroschritt festzulegen ist:

Abb. 48: Auswählen der Einfügeposition

Die gewünschte Position ist auszuwählen und durch Drücken der 'OK' Schaltfläche zu bestätigen. Daraufhin wird der gewünschte Makroschritt an der entsprechenden Position im Makro eingefügt und steht zur anschließenden Bearbeitung zur Verfügung.

Löschen

Mit dieser Schaltfläche können die markierten Makroschritte gelöscht werden. Es ist darauf zu achten, dass keine internen Makroschritte wie z. B. Informationen bzgl. der Makrosteuerung gelöscht werden. Dies sollte nur in begründeten Ausnahmefällen geschehen. Es ist zu beachten, dass das Löschen von Steuerungsinformationen zu einer fehlerhaften Makroausführung führen kann.

Kopieren

Markierte Makroschritte können zum späteren Einfügen in eine interne Zwischenablage des Makroeditors kopiert werden. Insbesondere können damit auch Makroschritte zwischen verschiedenen Makros kopiert werden, falls mehrere Makros gleichzeitig zum Editieren geöffnet sind.

Einfügen

Sobald einer oder mehrere Makroschritte in die interne Zwischenablage kopiert wurden, wird die Schalfläche zum Einfügen aktiviert. Zum Einfügen ist ein gewünschter Makroschritt vor oder hinter der gewünschten Einfügeposition zu markieren und die Schaltfläche auszuwählen. Der Makroeditor erfragt daraufhin die Einfügeposition (vor oder nach der ausgewählten Zeile) und fügt schließlich die zuvor kopierten Schritte ein.

Speichern

Sobald Veränderungen an einem Makro vorgenommen wurden, aktiviert der Makroeditor diese Schaltfläche. Durch drücken werden sämtliche Veränderungen in der Makrodatei abgespeichert. Sollte der Anwender den Makroeditor schließen, während noch nicht gespeicherte Veränderungen existieren, erfolgt eine Nachfrage beim Anwender, ob die durchgeführten Veränderungen verworfen oder gespeichert werden sollen.

Undo/Redo

Durchgeführte Veränderungen an einem Makro können rückgängig gemacht werden und wieder hergestellt werden. Dies ist durch Auswahl der entsprechenden Schaltflächen aus der Toolbar durchzuführen. Diese Möglichkeit besteht auch für Editierschritte, die vor dem Abspeichern des momentan bearbeiteten Makros durchgeführt wurden.

Fallbeispiel

Das oben gezeigte Beispielmakro soll so verändert werden, dass der Anwender bei der Ausführung des Makros nach dem Namen der Region gefragt wird, die angezeigt werden soll. Dafür gibt es verschiedene Möglichkeiten.

Editieren des Makros

Die erste Möglichkeit besteht darin, die entsprechende Texteingabe 's jes2' zunächst zu kopieren und dann direkt hinter dem bereits bestehenden Schritt einzufügen und somit zu verdoppeln. Daraufhin ist die Texteingabe für den originalen Schritt auf 's ' zu verkürzen und die Texteingabe für den kopierten Schritt auf 'jes2' zu reduzieren. Damit ist ein Split der ursprünglich zusammenhängenden Eingabe erreicht worden.

Im neu hinzugefügten zweiten Schritt ist nun noch in der letzten Spalte ('Nachfragen') das Attribut 'ja' zu wählen. Danach besteht das Makro aus den folgenden Schritten:

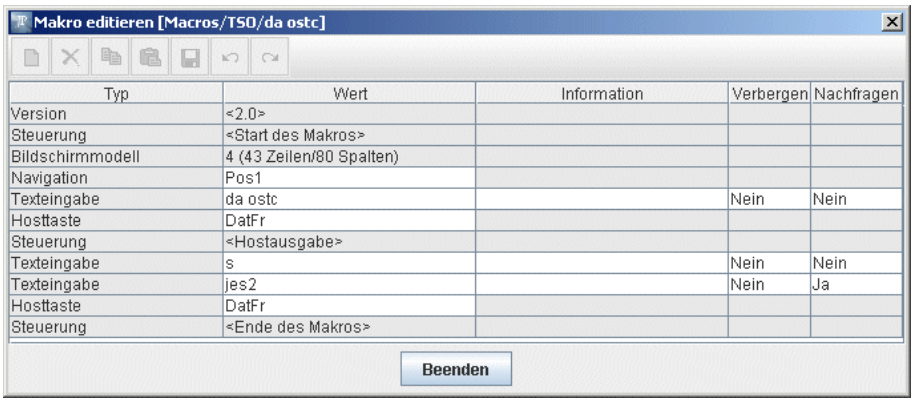


Abb. 49: Das bearbeitete Makro

Sobald das Makro ausgeführt wird, erfragt JProtector durch Einblendung des nachfolgend abgebildeten Dialogs den gewünschten Wert für die Eingabe. Der Wert ist mit der ursprünglichen Eingabe 'jes2' vorbelegt:

Abb. 50: Nachfrage für die Texteingabe

Der Anwender kann nun den gewünschten Namen der anzuzeigenden Region wählen und durch Drücken der Schaltfläche 'OK' oder der Returntaste seine Auswahl bestätigen. JProtector fährt daraufhin mit der Ausführung des Makros unter Verwendung der vom Benutzer gemachten Eingabe fort.

Split der Texteingabe während der Aufzeichnung

JProtector bietet noch eine alternative Möglichkeit, um den zuvor durch Bearbeitung des Makros beschriebenen Effekt zu erzielen.

Wenn der Anwender schon während der Aufzeichnung des Makros weiß, dass bestimmte Texteingaben variabel sein sollen, kann er während der Aufzeichnung bereits einen Split von zusammenhängenden Texteingaben erzwingen.

Dazu stellt JProtector eine Funktion bereit, die einer Tastenkombination im Rahmen der Verwaltung der Tastaturbelegung zugeordnet werden kann. Die nachfolgende Abbildung zeigt eine mögliche Zuordnung:

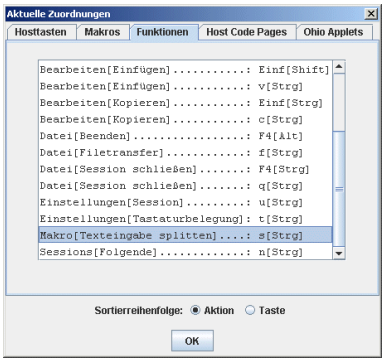


Abb. 51: Zuordnung der Funktion 'Makro – Texteingabe splitten'

Wenn z. B. die oben gezeigte Zuordnung erfolgt ist, kann der Anwender während der Aufzeichnung des Makros durch Drücken der Tastenkombination Steuerung + s bewirken, dass JProtector die bis dahin aufgezeichnete Texteingabe beendet. Damit werden sich direkt anschließende weitere Texteingaben in einem neuen Makroschritt gespeichert. Dies kann während der Texteingabe beliebig oft erfolgen.

Die erneute Aufzeichnung des Beispielmakros unter Verwendung der geschilderten Funktion führt zu dem folgenden Ergebnis:

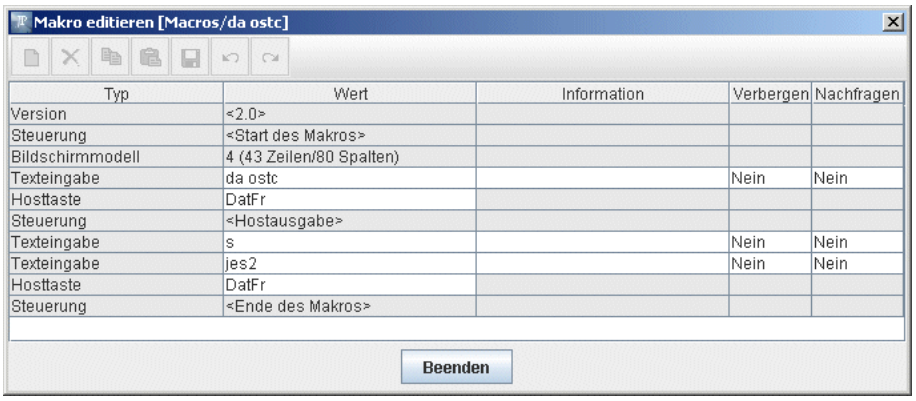


Abb. 52: Ergebnis der Aufzeichnung mit Split der Texteingabe

Damit das Verhalten des Makros wie gewünscht ist, ist abschließend noch für die entsprechende Texteingabe das Attribut für 'Nachfragen' auf 'Ja' zu setzen.

Verfügbare Schritttypen

Wie bereits zuvor gesehen unterscheidet JProtector verschiedene Schritttypen. Jeder Schritttyp führt zur Ausführung einer speziellen Aktion. Die nachfolgende Tabelle listet alle verfügbaren Schritttypen auf.

Schritttyp	**Beschreibung**
Texteingabe	Simulation von Texteingaben analog zur Eingabe über die Tastatur.
Navigation	Navigation der Einfügemarke. Mit diesem Typ kann z. B. das Drücken der Taste 'Links' simuliert werden.
Hosttaste	Auslösen einer Host Interrupttaste. Dieser Makroschritt führt zum Austausch von Informationen zwischen JProtector und dem verbundenen Host.
Wait	Pausieren der Makroausführung für ein festgelegtes Intervall.
Ausschneiden	Simulation der gleichnamigen Aktion für die Zwischenablage.
Kopieren	Simulation der gleichnamigen Aktion für die Zwi
Einfügen	Simulation der gleichnamigen Aktion für die Zwi

Anfügen	Simulation der gleichnamigen Aktion für die Zwi
Markierten Bereich setzen	Festlegen des Markierten Bereichs unter Angabe des linken oberen und rechten unteren Eckpunktes.
Alles markieren	Markieren des gesamten Inhalts des Emulationsfensters.
Mausklick	Simulation eines Mausklicks auf das Zeichen, das sich am angegebenen Punkt des Emulationsfensters befindet. Die Angabe wird als Zeile/Spalte interpretiert.
Maus Doppelklick	Simulation eines Doppelklicks mit der Maus auf das Zeichen, das sich am angegebenen Punkt des Emulationsfensters befindet. Die Angabe wird als Zeile/Spalte interpretiert.
Eingabemarke positionieren	Positionierung der Eingabemarke auf die angegebene Bildschirmposition. Die Angabe wird als Zeile/Spalte interpretiert.

Kapitel

12

Tastaturbelegung

Die Möglichkeit der individuellen Anpassung der Tastaturbelegung durch den Benutzer ist bei der Arbeit mit einer Terminalemulation ein wichtiger Punkt.

Der Verwaltungsdialog

Mit Hilfe des nachfolgend abgebildeten Dialogs kann eine beliebige Anzahl von Tastaturbelegungen verwaltet werden. Der Dialog ist unter Verwendung des Menüpunktes 'Verwaltung::Tastaturbelegungen' anzuzeigen.

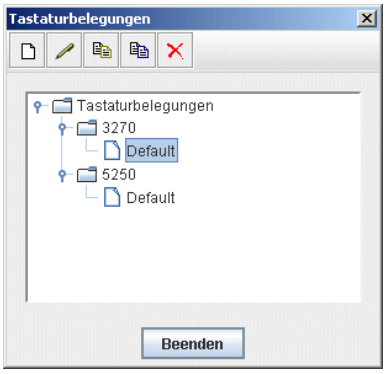


Abb. 53: Verwaltung der Tastaturbelegungen

Neu

Mit dieser Schaltfläche können neue Tastaturbelegungen erstellt werden.

Bearbeiten

Um die markierte Tastaturbelegung zu bearbeiten, ist diese Schaltfläche auszuwählen oder in der Baumansicht ein Doppelklick auf dem gewünschten Eintrag auszuführen.

Umbenennen

Diese Schaltfläche dient zum Umbenennen der in der Baumansicht markierten Tastaturbelegung.

Kopieren

Unter Verwendung dieser Schaltfläche kann eine Kopie der selektierten Tastaturbelegung erstellt werden.

Löschen

Zum Löschen einer Tastaturbelegung ist diese in der Baumansicht zu selektieren und diese Schaltfläche auszuwählen. Der Versuch, eine Tastaturbelegung zu löschen, die von mindestens einer Session verwendet wird, wird von JProtector abgewiesen.

Der Tastaturbelegungsdialog

JProtector stellt dem Benutzer zum Bearbeiten der Tastaturbelegung einen komfortablen Dialog zur Verfügung. Der Dialog kann durch Auswahl des Menüpunktes 'Einstellungen::Tastaturbelegung' eingeblendet werden. Damit wird die Bearbeitung der Tastaturbelegung ermöglicht, die in der aktiven Session verwendet wird. Die allgemeine Verwaltung der Tastaturbelegungen erfolgt unter Verwendung des Menüpunktes 'Verwaltung::Tastaturbelegungen'.

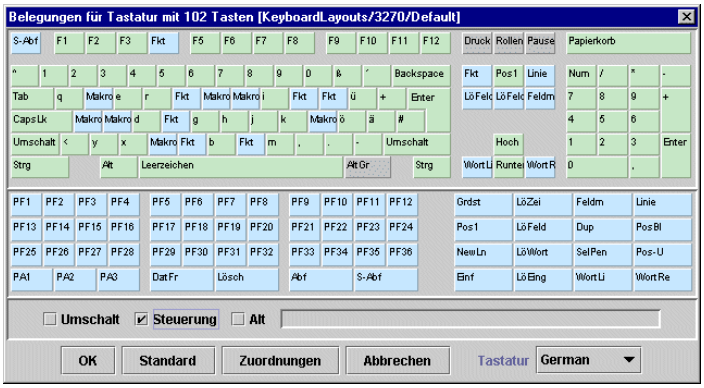


Abb. 54: Tastaturbelegung 3270

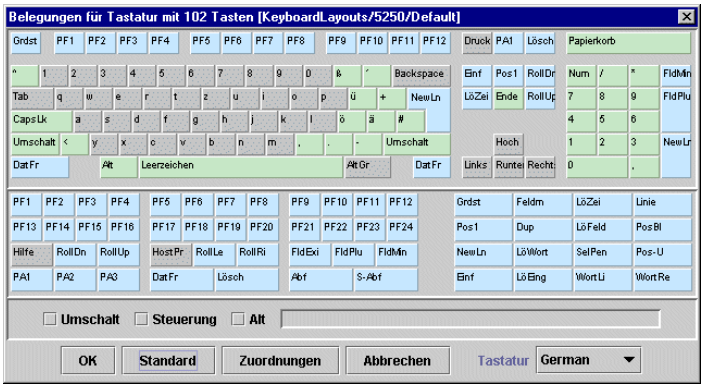


Abb. 55: Tastaturbelegung 5250

Allgemein

Der Dialog enthält im oberen Bereich die Abbildung einer PC Tastatur. Bereits mit einer Funktionalität belegte Tasten sind hellblau dargestellt. Tasten, für die eine Zuweisung erfolgen kann, sind hellgrün abgebildet. Tasten, denen keine Funktion zugewiesen werden kann, erscheinen in hellgrau.

Im mittleren Bereich des Dialogs befindet sich eine Liste der von JProtector unterstützten Hosttasten. Hosttasten, denen bereits eine Taste(nkombination) zugewiesen ist, sind in hellblau dargestellt. Wenn eine Hosttaste nicht über die Tastatur ausgelöst werden kann, ist sie in hellgrau dargestellt.

Darunter befinden sich Kontrollkästchen für die Aktivierung der möglichen Sondertasten. Die entsprechenden Kontrollkästchen sind zu selektieren, um die Belegung für gedrückte Sondertasten anzuzeigen.

Daneben befindet sich ein Anzeigefeld, in dem die aktuelle Belegung einer PC Taste angezeigt wird, wenn der Mauszeiger über die Taste im oberen Dialogbereich bewegt wird.

Zuweisung einer Hosttaste

Die Zuweisung einer Hosttaste an eine Taste(nkombination) erfolgt am einfachsten durch Drag und Drop. Dazu ist die zuzuweisende Hosttaste im mittleren Bereich des Dialogs mit gedrückter linker Maustaste in den PC Tastenbereich zu ziehen und über der gewünschte Taste fallenzulassen, indem die Maustaste losgelassen wird. Die erfolgte Zuweisung wird sofort durch eine veränderte Beschriftung der PC Taste angezeigt.

Wenn die Hosttaste der Kombination einer Taste mit einer oder mehreren Sondertasten zugewiesen werden soll, sind die gewünschten Sondertasten vorher durch Selektion der entsprechenden Kontrollkästchen festzulegen.

Während des Drag und Drop Vorganges werden die selektierte Hosttaste weiß und mögliche Zieltasten dunkelblau dargestellt.

Eine Hosttaste kann beliebig vielen Tasten(kombinationen) zugewiesen werden. Um alle Zuweisungen für eine Hosttaste zu löschen, ist die Hosttaste mittels Drag und Drop auf den Papierkorb im rechten oberen Bereich des Dialogs zu ziehen.

Entsprechend kann die für eine PC Taste erfolgte Zuweisung gelöscht werden, indem die PC Taste mittels Drag und Drop auf den Papierkorb gezogen wird.

Andere Möglichkeiten der Tastaturbelegung

JProtector bietet darüber hinaus auch die Möglichkeit, sämtliche Menüfunktionen, die Ausführung aufgezeichneter Makros, die Ausführung von Ohio / Oska Applets sowie die Selektion von Host Code Pages mit dem Drücken einer Taste(nkombination) zu verbinden.

Dazu sind zunächst die gewünschten Sondertasten zu aktivieren. Danach ist auf der PC Taste, für die eine Zuweisung erfolgen soll, ein Doppelklick mit der Maus auszuführen. Im daraufhin eingeblendeten Dialog kann eine Zuweisung erfolgen oder eine bestehende Zuweisung durch Auswahl der Schaltfläche 'keine' gelöscht werden.

Tastenzuweisung – Hosttasten

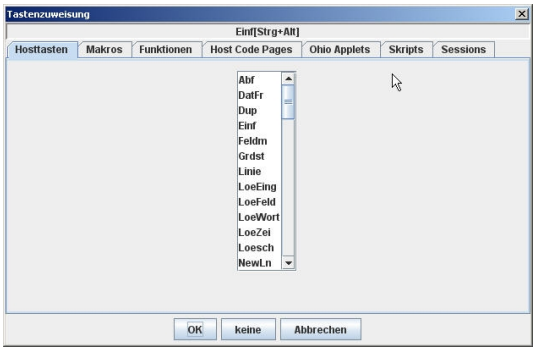


Abb. 56: Tastenzuweisung - Hosttasten

Diese Dialogseite bietet eine alternative Möglichkeit, eine Hosttaste einer Tastenkombination zuzuweisen. Dazu ist die gewünschte Hosttaste aus der Auswahlliste zu selektieren und der Dialog durch Drücken der Schaltfläche 'OK' zu beenden.

Tastenzuweisung – Makros

Die nachfolgend abgebildete Dialogseite zeigt ein Baumdiagramm, das alle momentan verfügbaren Makros enthält.

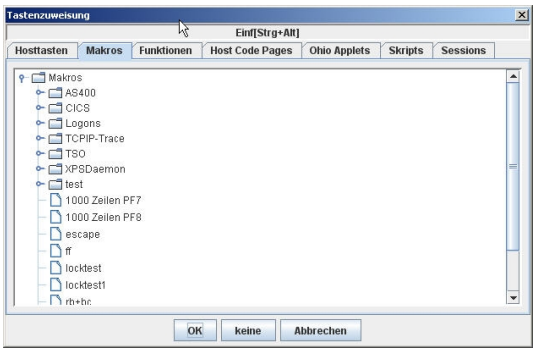


Abb. 57: Tastenzuweisung - Makros

Die Zuweisung des Makros erfolgt entweder durch Selektion des Makros im Baum und anschließendes Drücken der Schaltfläche 'OK' oder durch Doppelklicken mit der Maus auf den Makronamen.

Tastenzuweisung – Funktionen

Die Belegung einer PC Taste(nkombination) mit einer Menüfunktion erfolgt unter Verwendung der folgenden Dialogseite:

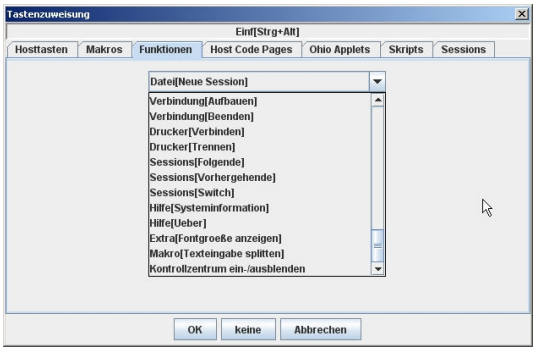


Abb. 58: Tastenzuweisung - Funktionen

Die Zuordnung einer Menüfunktion erfolgt über Selektion der Funktion aus der Auswahlliste und anschließendes Drücken der Schaltfläche 'OK'.

Tastenzuweisung - Host Code Pages

Mitunter kann es sich als nützlich erweisen, die zur Zeichenumsetzung verwendete Host Code Page zu verändern. Dies ist z. B. beim Schreiben von C-Programmen der Fall. Damit die in 'C' verwendeten Sonderzeichen korrekt dargestellt werden, ist die Verwendung der Host Code Page USA (international) notwendig. Das verhindert jedoch die korrekte Anzeige von deutschen Sonderzeichen, wie etwa ü, ö oder ä. Um die verwendete Host Code Page auf einfache Weise zu wechseln, kann die Aktivierung einer Host Code Page mit dem Drücken einer Taste(nkombination) verbunden werden. Dies erfolgt über den folgenden Dialog:

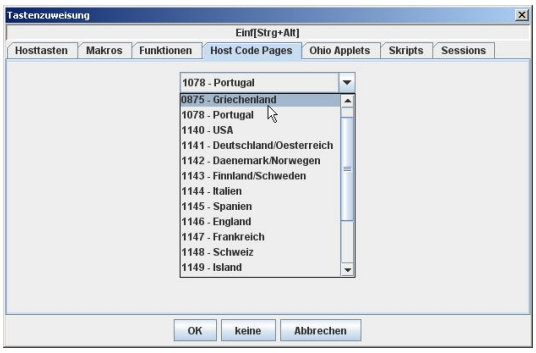


Abb. 59: Tastenzuweisung - Host Code Pages

Die Zuordnung einer Host Code Page erfolgt über Selektion der Host Code Page aus der Auswahlliste und anschließendem Drücken der Schaltfläche 'OK'.

Tastenzuweisung - Ohio Applets

Ohio Applets sind Java Programme, die von JProtector im Kontext einer Emulationssession gestartet werden. Ohio Applets können verschiedenste Aufgaben übernehmen und Einfluss auf die Emulationssession nehmen. Die Zuweisung der Ausführung eines Ohio Applets an eine Taste(nkombination) erfolgt mit der nachfolgend abgebildeten Dialogseite:

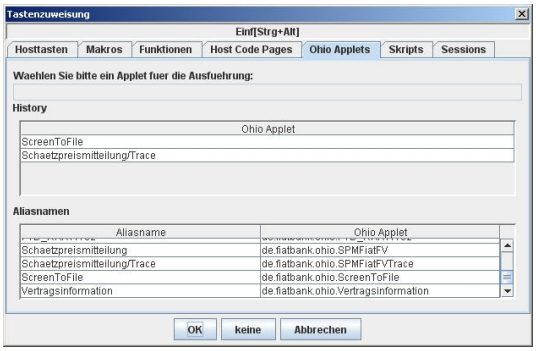


Abb. 60: Tastenzuweisung - Ohio Applets

Das zuzuordnende Ohio Applet kann durch Auswahl eines Eintrages aus der History-Liste oder aus der Tabelle der Aliasnamen selektiert werden.

Tastenzuweisung - Scripts

JProtector ermöglicht die Ausführung von Scripts, die z. B. in JavaScript oder in Groovy geschrieben wurden. Scripts können über die Ohio Programmierschnittstelle auf den Inhalt des Emulationsfensters zugreifen bzw. Funktionen wie z. B. das Auslösen einer Interrupttaste ausführen.

Die Zuweisung der Ausführung eines Scripts an eine Taste(nkombination) erfolgt mit der nachfolgend abgebildeten Dialogseite:

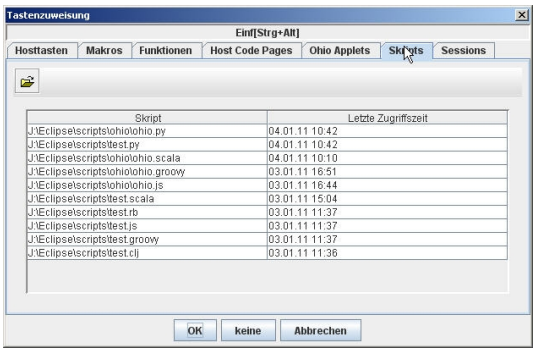


Abb. 61: Tastenzuweisung - Scripts

Das zuzuordnende Script ist in der aufgelisteten Tabelle der bekannten Scripts zu selektieren.

Tastenzuweisung - Sessions

JProtector ermöglicht die Aktivierung einer Session über das Drücken eines Hotkeys.

Die Zuordnung eines Hotkey für die Aktivierung einer Session an eine Taste(nkombination) erfolgt mit der nachfolgend abgebildeten Dialogseite:

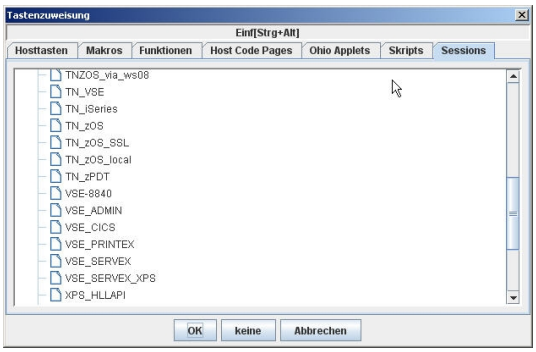


Abb. 62: Tastenzuweisung - Sessions

Die zuzuordnende Session ist aus der Liste der definierten Sessions auszuwählen.

Weitere Funktionen

Der Tastaturbelegungsdialog stellt noch eine Reihe weiterer Funktionen zur Verfügung, die nachfolgend beschrieben werden.

Anzeige einer gedrückten Taste

Während der Anzeige des Dialogs erfolgt beim Drücken einer beliebigen PC Taste die farbliche Hervorhebung der Taste (dunkelblau) in der Anzeige der PC Tastatur.

Wiederherstellung der Standardbelegung

Wenn die nach der Installation standardmäßig vorgegebene Tastaturbelegung wiederhergestellt werden soll, kann dies durch Drücken der Taste 'Standard' geschehen. Damit gehen jedoch alle zwischenzeitlich vorgenommenen Veränderungen an der Tastaturbelegung verloren. Es sei darauf hingewiesen, dass vorgenommene Veränderungen ausschließlich bei Verlassen des Dialogs durch Drücken der 'OK' Taste aktiv werden. Andernfalls bleibt die vor Einblendung des Dialogs aktive Belegung erhalten.

Auswahl der Tastatursprache

Die Auswahlliste im rechten unteren Bereich des Dialogs enthält eine Reihe von verschiedenen Sprachen, die für die Darstellung der PC Tastaturbelegung verwendet werden können. Es empfiehlt sich, die Sprache zu selektieren, die im Rahmen der Einstellungen im Betriebssystem für die Tastatur vergeben wurde. Die hier ausgewählte Sprache hat lediglich einen Einfluss auf die Darstellung der PC Tastatur im Dialog. Sie ist bei der Verarbeitung von Tastatureingaben durch JProtector ohne Bedeutung.

Anzeige der aktiven Zuordnungen

Es kann sich als hilfreich erweisen, festzustellen, welche Tastenzuordnungen momentan aktiv sind. Dazu kann ein Anzeigedialog durch Drücken der Schaltfläche 'Zuordnungen' eingeblendet werden.

Dieser Dialog enthält Seiten, auf denen die bestehenden Zuordnungen für Hosttasten, Makros, Funktionen, Host Code Pages und Ohio Applets angezeigt werden.

Durch Selektion der entsprechenden Radioschaltfläche im unteren Bereich des Dialogs kann die Sortierreihenfolge der Anzeige zwischen 'Aktion' und 'Taste' umgeschaltet werden.

Aktuelle Zuordnungen - Hosttasten

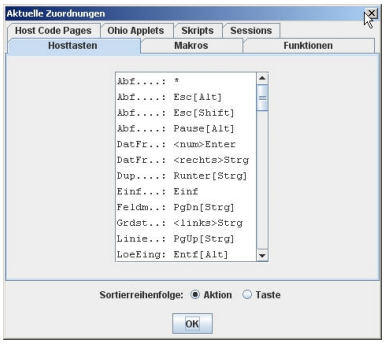


Abb. 63: Aktuelle Zuordnungen - Hosttasten

Die Dialogseite zeigt die aktuelle Belegung von PC Tasten mit Hosttasten.

Aktuelle Zuordnungen – Makros

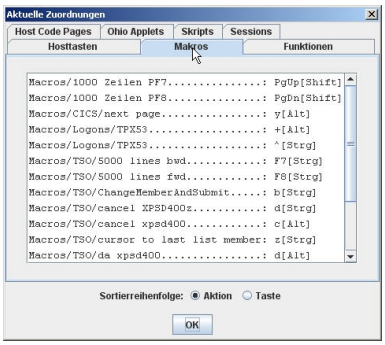


Abb. 64: Aktuelle Zuordnungen - Makros

Die aktuelle Zuweisung von Makros an PC Tasten ist dieser Dialogseite zu entnehmen.

Aktuelle Zuordnungen – Funktionen

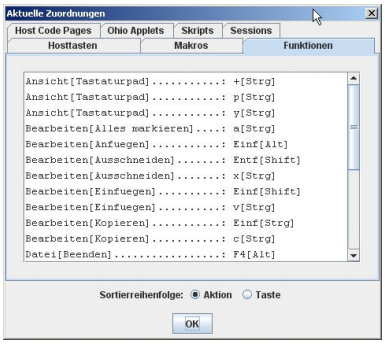


Abb. 65: Aktuelle Zuordnungen - Funktionen

Diese Dialogseite zeigt die Zuweisungen von JProtector Menüfunktionen an Tasten(kombinationen) der PC Tastatur.

Aktuelle Zuordnungen - Host Code Pages

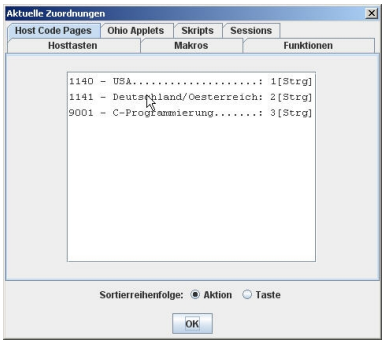


Abb. 66: Aktuelle Zuordnungen - Host Code Pages

Dieser Dialogseite ist die Zuordnung von Host Code Pages zu Tasten(kombinationen) zu entnehmen.

Aktuelle Zuordnungen – Ohio Applets

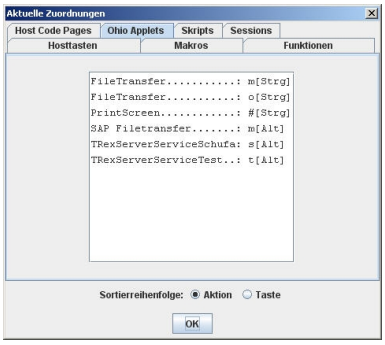


Abb. 67: Aktuelle Zuordnungen - Ohio Applets

Diese Dialogseite zeigt die Verknüpfung von Tasten(kombinationen) mit der Ausführung von Ohio Applets an.

Aktuelle Zuordnungen – Scripts

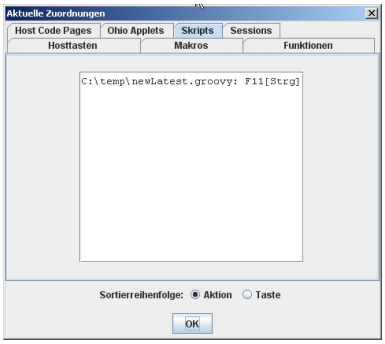


Abb. 68: Aktuelle Zuordnungen - Ohio Applets

Diese Dialogseite zeigt die Verknüpfung von Tasten(kombinationen) mit der Ausführung von Scripts an.

Aktuelle Zuordnungen – Sessions

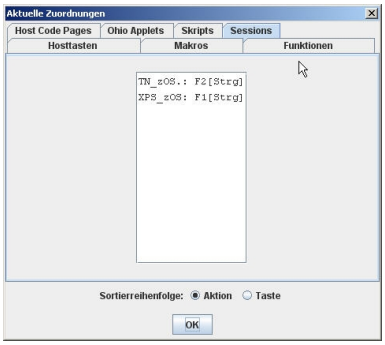


Abb. 69: Aktuelle Zuordnungen - Sessions

Diese Dialogseite zeigt die Verknüpfung von Tasten(kombinationen) mit der Aktivierung aktiver Sessions an. Die Aktivierung kann nur für bereits geöffnete Sessions erfolgen.

Kapitel

13

Farbschemata

Um die Verwaltung der Oberflächengestaltung eines JProtector Sessionfensters zu vereinfachen, ermöglicht JProtector den Einsatz von Farbschemata. Jedes Farbschema enthält Definitionen für die Anzeige der verschiedenen Ausgabefarben. Außerdem wird hier festgelegt, ob das Emulationsfenster mit einem '3D-Effekt' versehen werden soll, und in welcher Farbe der nicht vom Emulationsfenster benötigte Bereich dargestellt werden soll.

Die allgemeine Verwaltung von Farbschemata erfolgt mit dem folgenden Dialog, der durch Auswahl des Menüpunktes 'Verwaltung::Farbschemata' eingeblendet wird.

Der Verwaltungsdialog

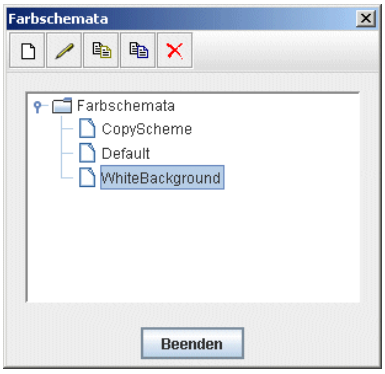


Abb. 70: Verwaltung der Farbschemata

Neu

Mit dieser Schaltfläche kann ein neues Farbschema erstellt werden.

Bearbeiten

Um das ausgewählte Farbschema zu bearbeiten, ist diese Schaltfläche auszuwählen oder in der Baumansicht ein Doppelklick auf dem gewünschten Eintrag auszuführen.

Umbenennen

Diese Schaltfläche dient zum Umbenennen des in der Baumansicht markierten Farbschemas.

Kopieren

Unter Verwendung dieser Schaltfläche kann eine Kopie des markierten Farbschemas erstellt werden.

Löschen

Zum Löschen eines Farbschemas ist dieses in der Baumansicht zu selektieren und diese Schaltfläche auszuwählen. Der Versuch, ein Farbschema zu löschen, das in mindestens einer Session verwendet wird, wird von JProtector abgewiesen.

Der Farbschemadialog

Die Bearbeitung eines Farbschemas erfolgt mit Hilfe des nachfolgend abgebildeten Dialogs. Dieser Dialog ist durch Auswahl des Menüpunktes 'Einstellungen::Farbschema' anzuzeigen, was die Bearbeitung des Farbschemas für die aktive Session ermöglicht. Die allgemeine Verwaltung von Farbschemas erfolgt durch Auswahl des Menüpunktes 'Verwaltung::Farbschemata'.

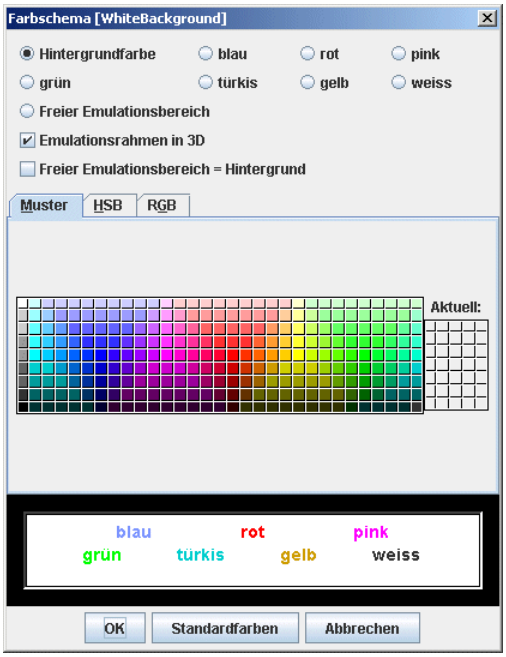


Abb. 71: Farbschema – feste Farben

Farbauswahl

Im oberen Bereich des Dialogs ist die Farbe bzw. der Bereich auszuwählen, für den eine Farbzuweisung erfolgen soll. Unter dem 'freien Emulationsbereich' ist der Bereich des Fensters zu verstehen, der das Emulationsfenster direkt umschließt, aber nicht für die Maskendarstellung verwendet wird. Die Größe dieses Bereiches kann durch eine Veränderung der Fenstergröße und der daraus resultierenden Veränderung der Zeichensatzgröße variiert werden. Siehe auch 'Freier Emulationsbereich = Hintergrund'.

Emulationsrahmen in 3D

Mit diesem Auswahlkästchen kann festgelegt werden, ob der Ausgabebereich für die Emulationsanzeige einen dreidimensionalen Rahmen erhalten soll.

Freier Emulationsbereich = Hintergrund

Hier ist festzulegen, ob der freie Emulationsbereich in derselben Farbe wie der Emulationshintergrund erscheinen soll.

Farbauswahl

Dieser Teil des Dialogs dient zur Festlegung der darzustellenden Farben. Eine getroffene Farbauswahl für den gewählten Parameter wird sofort in der unterhalb liegenden Vorschau angezeigt. Der Dialog enthält neben einer Tabelle fester Farbwerte weitere Seiten zur Festlegung der Farben:

HSB (Hue/Saturation/Brightness)

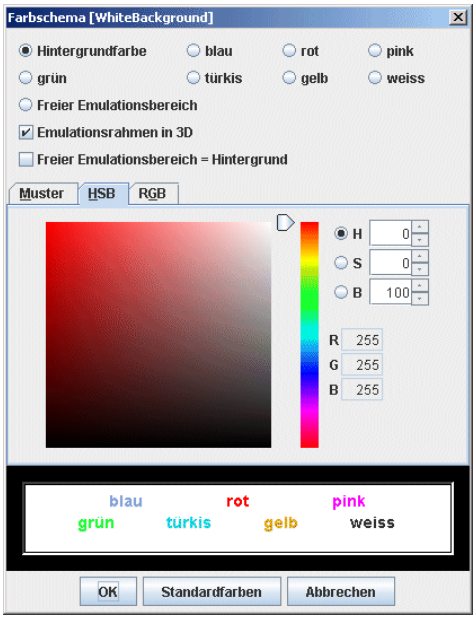


Abb. 72: Farbschema - HSB

RGB (Red/Green/Blue)

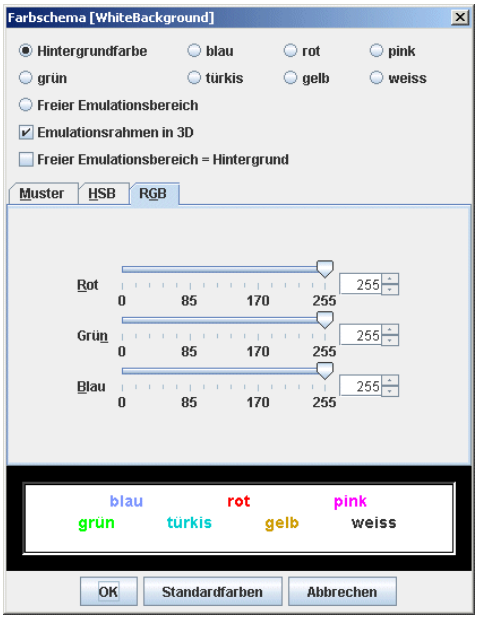


Abb. 73: Farbschema - RGB

Standardfarben

Mit dieser Schaltfläche kann das Farbschema auf Standardwerte zurückgesetzt werden. Diese Standardwerte werden von JProtector vorgegeben.

Kapitel

14

Ohio/Oska

Die Integration bestehender Hostapplikationen in moderne Geschäftsabläufe erfordert es, dass eine Terminalemulation Programmierschnittstellen zur Verfügung stellt, die es auf einfache Weise ermöglichen, den Ablauf einer Emulationssession über Programme zu beeinflussen oder sogar komplett zu steuern.

Zu diesem Zweck stellt JProtector das Ohio/Oska API zur Verfügung. Ohio, das für 'Open Host Interface Objects' steht, ist ein Pseudostandard für ein objektorientiertes API zur Steuerung einer Emulationssession. Neben dem Ohio API stellt die XPS Software GmbH zusätzlich noch das Oska API zur Verfügung. Oska steht für 'Ohio Skeleton Automat' und ist eine Erweiterung des Ohio APIs, die dem Entwickler verschiedene, wiederkehrende Routineaufgaben, wie etwa die Identifizierung angezeigter Hostmasken, abnimmt. Die detaillierte Beschreibung der verschiedenen APIs ist Bestandteil eines eigenen Handbuches.

JProtector fasst unter dem Menüpunkt 'Ohio' verschiedene Funktionen zur Entwicklungsunterstützung und Ausführung von Ohio/Oska Applets zusammen.

Ausführung von Applets

Im Rahmen einer Terminalsession können Ohio/Oska Applets auf verschiedene Weise ausgeführt werden.

Eine Möglichkeit besteht darin, die Ausführung eines Applets mit dem Drücken einer definierten Tastenkombination zu verknüpfen. Eine Beschreibung zur Vorgehensweise findet sich im Kapitel 'Tastaturbelegung' auf Seite 77.

Eine weitere Möglichkeit besteht darin, ein Applet direkt für die Ausführung auszuwählen. Dazu ist durch Auswahl des Menüpunkts 'Ohio::Ohio Applet ausführen' der nachfolgend abgebildeten Dialog einzublenden, in dem das auszuführende Applet selektiert werden kann:

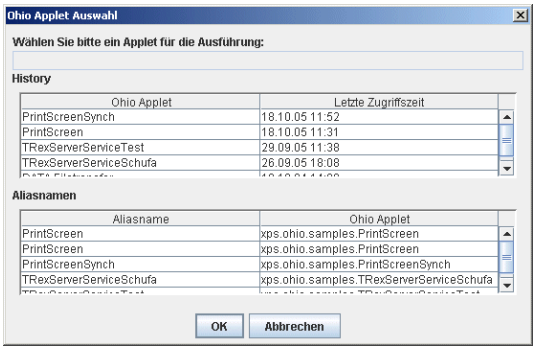


Abb. 74: Ohio Applet Auswahl

Das gewünschte Applet kann aus der History-Liste oder aus der Tabelle der Aliasnamen ausgewählt werden. Die Ausführung erfolgt unmittelbar nach Beendigung des Dialogs mit der 'OK' Schaltfläche.

Des Weiteren enthält das 'Ohio' Menü eine Liste der zuletzt ausgeführten Applets, aus der ebenfalls ein Applet zur Ausführung ausgewählt werden kann.

Ohio Anzeigemodus

JProtector erlaubt das Umschalten der Maskenanzeige in den Ohio Anzeigemodus. Dieser Modus erleichtert die Ermittlung von Informationen zur angezeigten Maske. Dies geschieht zum einen durch die farbliche Darstellung. Attributpositionen werden revers, geschützte Schirmpositionen grün und ungeschützte blau dargestellt. Außerdem wird in der Statuszeile immer die Zeile / Spalte angezeigt, über der sich der Mauszeiger momentan befindet. Die Emulation kann im Ohio Anzeigemodus unverändert bedient werden.

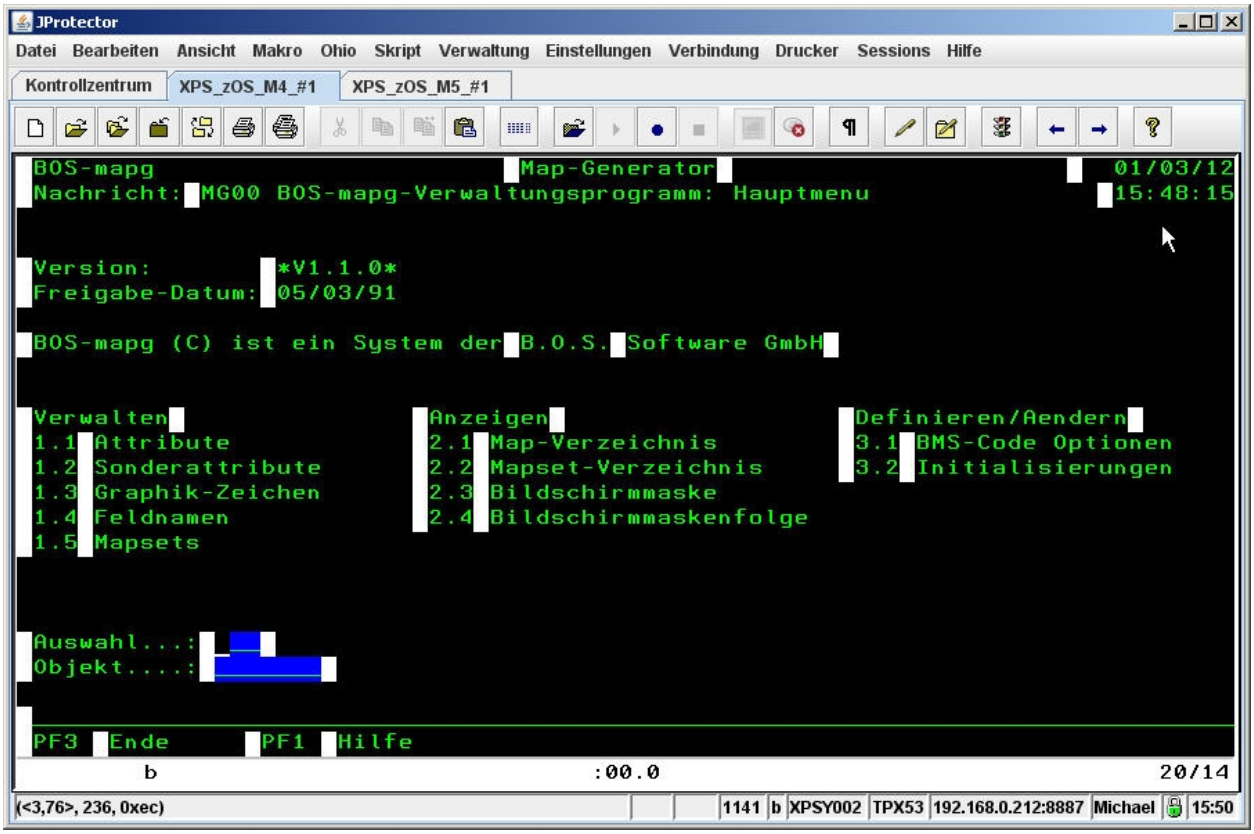


Abb. 75: Ohio Anzeigemodus

Kapitel

15

Skripts

Eine der Richtungen, in die die Weiterentwicklung der Java Virtual Machine fortschreitet, ist die Unterstützung weiterer Sprachen. In diesem Zusammenhang werden bereits eine Reihe moderner Skriptsprachen von der Java VM unterstützt.

JProtector ermöglicht dem Benutzer die Ausführung von Skripts im Rahmen einer JProtector Terminalsession. Momentan werden die folgenden Skriptsprachen unterstützt:

Skriptsprache	Beschreibung	Dateiendung	Script-Engine
Groovy	Java-ähnliche Skriptsprache mit einfacher Integration bestehender Java-Klassen.	.groovy	groovy.jar
JavaScript (ECMAScript)	Implementierung von der Skriptsprache JavaScript für die Java VM. Bestehende Java-Klassen können integriert werden.	.js	bereits in der Java VM enthalten
JRuby	Implementierung der Skriptsprache Ruby für die Java VM. Bestehende Java-Klassen können integriert werden.	.rb	jruby.jar
Jython	Implementierung der Skriptsprache Python für die Java VM. Bestehende Java-Klassen können integriert werden.	.py	jython.jar

Damit JProtector ein Skript, das in der jeweiligen Sprache geschrieben ist, ausführen kann, ist sicherzustellen, dass der Name der Datei, die den Quelltext des Skripts enthält, die erforderliche Endung hat.

Darüber hinaus sind die entsprechenden Vorkehrungen zur Installation der jeweiligen Script-Engine zu treffen. Die benötigten JSR223 Skript-Engines sind Teil der JProtector Distribution. Die Script-Engines selbst sind vor der Nutzung zu installieren. Lediglich JavaScript ist bereits integrierter Teil der neueren Java Virtual Machines.

Vor Ausführung eines Skripts in der gewünschten Sprache ist dafür zu sorgen, dass der benötigte Skriptprozessor aus dem Klassenpfad geladen werden kann. Am einfachsten kann dies erreicht werden, in dem der Skriptprozessor (groovy.jar, jruby.jar, jython.jar) in das 'lib'-Verzeichnis der eingesetzten Java Virtual Machine kopiert wird. Damit steht der Skriptprozessor nach dem Start der Java VM allen Applikationen zur Verfügung.

Die Ausführung von Skripts unter der Kontrolle von JProtector eröffnet ein weites Feld flexibler Anwendungsmöglichkeiten. Da die unterstützten Skriptsprachen die Einbindung bestehender Java-Klassen ermöglichen, können Skripts auf einfache Weise auf die von JProtector bereitgestellte Ohio Funktionalität zugreifen und damit zur Steuerung einer Emulations-Session eingesetzt werden. Das nachfolgend abgebildete Groovy-Skript soll diesen Punkt illustrieren.

Groovy

```
01 import xps.jprotector.*
02
03 println("Launching ohio.groovy")
04 ohioSession = new OhioSession("XPS_II", "XPS_II", false)
05 ohioScreen  = ohioSession.getScreen()
06 ohioScreen.setString("3", new OhioPosition(22,10))
07 ohioScreen.sendAid(Ohio.OHIO_AID_ENTER, true)
08 println("Terminating ohio.groovy")
```

Abb. 76: Groovy Skript mit Ohio Funktionalität

Durch die Einbindung des JProtector Ohio-Apis mit Hilfe des Statements 'import xps.jprotector.*' in Zeile 1 steht dem Skript das gesamte Ohio Interface zur Verfügung.

In den Zeilen 4 und 5 erfolgt zunächst der Zugriff auf die OhioSession mit dem Namen 'XPS_II' und daraufhin der Zugriff auf deren 3270 Bildschirm. Der Befehl auf Zeile 6 fügt zunächst die Menüauswahl '3' an der Schirmposition Zeile 22, Spalte 10 ein. In Zeile 7 wird schließlich das Drücken der Datenfreigabe-Taste veranlasst. Die Zeilen 3 und 8 schreiben Informationen auf die Systemkonsole. Auf die Bearbeitung von Fehlerfällen wurde zu Gunsten der Übersichtlichkeit verzichtet.

Dieses Beispiel zeigt auf einfache Weise, wie Skripts zur dynamischen Erweiterung von JProtector eingesetzt werden können. Insbesondere ist hier zu bedenken, dass der Quellcode für ein Skript in einer beliebigen Umgebung, z. B. durch ein VBA-Makro unter Microsoft Excel, generiert werden kann.

Somit ist die dynamische Erstellung von Skripts für die Ausführung einer Liste von File-Transfers zum Host oder die Abarbeitung tabellarisch vorliegender Eingabedaten für Hostmasken möglich. Um nur einige zu nennen. Die Tatsache, dass die generierten Skripts vor der Ausführung nicht kompiliert werden müssen, erleichtert die Nutzung erheblich. Die nachfolgenden Abbildungen zeigen Listings desselben Skripts in den anderen unterstützten Skriptsprachen.

JavaScript

```
importPackage(Packages.java.lang);
importPackage(Packages.xps.jprotector);

System.out.println("Launching ohio.js");
var ohioSession = new OhioSession("XPS_II", "XPS_II", false);
var ohioScreen  = ohioSession.getScreen();
ohioScreen.setString("3", new OhioPosition(22,10));
ohioScreen.sendAid(Ohio.OHIO_AID_ENTER, true);
System.out.println("Terminating ohio.js");
```

Abb. 77: JavaScript Skript mit Ohio Funktionalität

JRuby

```
require "java"

include_class "xps.jprotector.Ohio"
include_class "xps.jprotector.OhioSession"
include_class "xps.jprotector.OhioScreen"
include_class "xps.jprotector.OhioPosition"

puts "Launching ohio.rb"
ohioSession = OhioSession.new("XPS_II", "XPS_II", false)
ohioScreen  = ohioSession.getScreen()
ohioScreen.setString("3", OhioPosition.new(22, 10))
# ohioScreen.sendAid(Ohio.OHIO_AID_ENTER, true)
ohioScreen.sendAid(44, true)
puts "Terminating ohio.rb"
```

Abb. 78: JRuby Skript mit Ohio Funktionalität

Jython

```
from xps.jprotector import *

print "Launching ohio.py"
ohioSession = OhioSession('XPS_II', 'XPS_II', 0)
ohioScreen  = ohioSession.getScreen()
ohioScreen.setString('3', OhioPosition(22,10))
ohioScreen.sendAid(Ohio.OHIO_AID_ENTER, 1)
print "Terminating ohio.py"
```

Abb. 79: Jython Skript mit Ohio Funktionalität

Einblendung der Systemkonsole

Für das Testen von Skripts empfiehlt sich die Ausgabe von Informationen auf die Systemkonsole. Damit können Statusinformationen auf einfache Weise sichtbar gemacht werden.

Da bei der Ausführung von JProtector die Systemkonsole normalerweise nicht sichtbar ist, kann diese durch Auswahl des Menüpunktes 'Skript::Konsole öffnen', wie die nachfolgend abgebildet, eingeblendet werden.

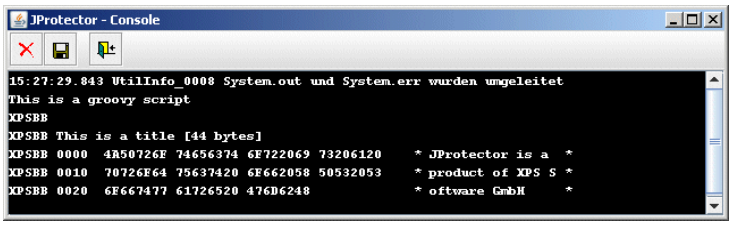


Abb. 80: JProtector - Konsole

Bei geöffneter Konsole werden alle Skript-Ausgaben auf System.out und System.err im Konsolenfenster angezeigt.

Ausführung eines Skripts

Die Ausführung eines Skripts kann auf zwei verschiedene Arten erfolgen.

Falls ein Skript zum ersten Mal ausgeführt wird, ist dazu der Menüpunkt 'Skript::Skript ausfuehren' auszuwählen. Im daraufhin eingeblendeten Datei-Auswahldialog kann das gewünschte Skript selektiert werden. Nach erfolgter Auswahl wird das Skript sofort ausgeführt.

JProtector speichert die Namen der letzten 8 ausgeführten Skripts in einer History-Liste, die sich im Skript-Menü befindet. Auswahl eines Skripts aus dieser History-Liste führt ebenfalls zur Ausführung des Skripts.

Die Auswahl der zugehörigen Skript-Engine erfolgt basierend auf der Dateiendung der gewählten Skriptdatei.

Verwaltung der History-Liste

Die History-Liste, in der bereits ausgeführte Skripts gespeichert werden, kann durch Auswahl des Menüpunkts 'Verwaltung::Skripts' verwaltet werden. Dazu kommt der nachfolgend abgebildete Dialog zum Einsatz:

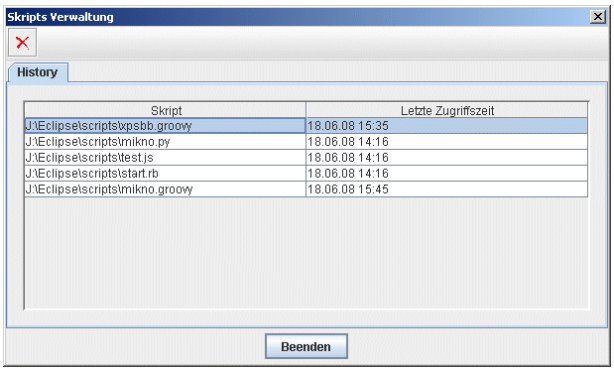


Abb. 81: Skripts Verwaltung

In der Liste der Skripts können ein oder mehrere Skripts markiert und anschließend durch Drücken der Taste gelöscht werden. Anschließend erscheinen die gelöschten Skripts nicht mehr in der History-Liste im Skript-Menü.

Kapitel

16

Konfigurierbare Werkzeugleisten

JProtector ermöglicht die Verwendung zusätzlicher Werkzeugleisten. Damit können dem Anwender im Kopfbereich des JProtector Emulationsfensters weitere Schaltflächen zur Verfügung gestellt werden, um z. B. Tastaturmakros oder Skripts mit einem Mausklick auszuführen.

Die Definition und Konfiguration weiterer Werkzeugleisten erfolgt innerhalb einer XML-Textdatei. Das Format der XML-Datei ist von XPS vorgegeben und wird im Weiteren beschrieben.

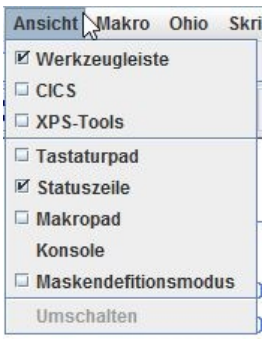
JProtector ist durch eine Angabe für die allgemeine Einstellung 'Datei mit zusaetzlichen Werkzeugleisten', wie auf Seite 30 beschrieben, über den Speicherort der Konfigurationsdatei zu informieren, die die Definitionen der zusätzlichen Werkzeugleisten enthält.

Der folgende Ausschnitt zeigt den grundsätzlichen Aufbau der Konfigurationsdatei:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<tool-bars>
  <tool-bar name="XPS-Tools">
    <item type="macro">
    </item>
  </tool-bar>
  <tool-bar name="CICS">
    <item type="script">
    </item>
  </tool-bar>
</tool-bars>
```

An die Standard XML-Kopfzeile schließt sich der '**<tool-bars>**' Bereich an, der als Kontainer für eine beliebige Anzahl von Werkzeugleisten dient.

Die Definition einzelner Werkzeugleisten erfolgt innerhalb des XML-Tags '**<tool-bar name="…">**'. Der gewählte Name für die Werkzeugleiste sollte eindeutig sein und wird, wie nachfolgend gezeigt, als eigener Eintrag in das 'Ansicht'-Menü der JProtector Terminalsessions aufgenommen:



Sollte für eine Toolbar in der XML-Datei der Name 'Standard' vergeben werden, dann werden die definierten Einträge der JProtector Standard Werkzeugleiste hinzugefügt.

Der Anwender kann eine oder mehrere zusätzliche Werkzeugleisten - analog zur Standard Werkzeugleiste - ein- und ausblenden. JProtector speichert den jeweils zuletzt gewählen Sichtbarkeitsstatus einer Werkzeugleiste und stellt diesen nach einem Neustart der Emulation wieder her.

Einzelne Elemente einer Werkzeugleiste werden durch je ein '**<item type="…">**' XML-Tag definiert.

JProtector stellt die folgenden Typen für Elemente der Werkzeugleiste zur Verfügung:

Separator

Ein Separator kann zum Einfügen eines Leerraumes zwischen 2 Elementen der Werkzeugleiste verwendet werden. Auf diese Weise können z. B. visuell abgesetzte Gruppen bestehend aus ähnlichen Funktionen erstellt werden.

Syntax

```
<item type="separator"/>
```

Hostkey

Elemente vom Typ 'hostkey' können zum Auslösen von Unterbrechungstasten wie z. B. der Funktions- oder PA-Tasten verwendet werden.

Syntax

```
<item type="hostkey">
  <view>
    <type>text</type>
    <value>PA2</value>
  </view>
  <action>
    <value>PA2</value>
  </action>
</item>
```

<table>
<tr><th>Option</th><th>Beschreibung</th></tr>
<tr><td><view><type></td><td>Mit dieser Option ist festzulegen, auf welche Weise JProtector das Element in der Werkzeugleiste darstellen soll. Folgende Angaben sind möglich:
<table>
<tr><th>Typ</th><th>Beschreibung</th></tr>
<tr><td>text</td><td>Die Darstellung des Elements erfolgt durch Text.</td></tr>
<tr><td>image</td><td>Die Darstellung des Elements erfolgt durch eine Grafik.</td></tr>
</table></td></tr>
<tr><td><view><value></td><td>Mit dieser Option ist der Wert für den zuvor gewählten Typen festzulegen.
<table>
<tr><th>Typ</th><th>Wert</th></tr>
<tr><td>text</td><td>Angabe des Textes, der auf der zugehörigen Schaltfläche der Werkzeugleiste angezeigt werden soll.</td></tr>
</table></td></tr>
</table>

	image	Angabe des voll qualifizierten Pfades zur Grafikdatei, die auf der zugehörigen Schaltfläche der Werkzeugleiste angezeigt werden soll. Unterstützte Typen sind '.gif' und '.jpg'.
<action><value>	Hier ist die Unterbrechungstaste anzugeben, die bei Auswahl der Schaltlfäche durch den Anwender an den Großrechner gesendet werden soll. Folgende Angaben sind zulässig: **CLEAR** **ENTER** **PF1 … PF36** **PA1 … PA3** **REQUEST** **SYSREQUEST**	

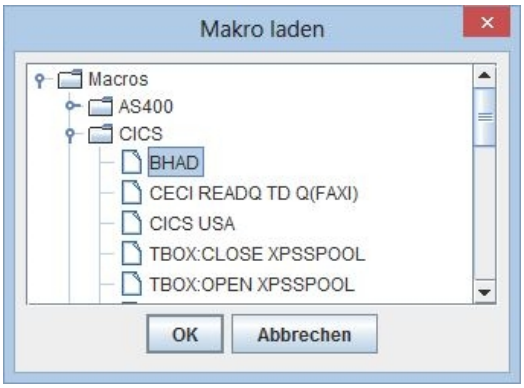
Makro

Elemente vom Typ 'macro' können zur Ausführung eines aufgezeichneten Tastaturmakros verwendet werden.

Syntax

```
<item type="macro">
  <view>
    <type>image</type>
    <value>j:\jprot\help.gif</value>
  </view>
  <action>
    <value>CICS/BHAD</value>
  </action>
</item>
```

Option	Beschreibung
<view><type>	Mit dieser Option ist festzulegen, auf welche Weise JProtector das Element in der Werkzeugleiste darstellen soll. Folgende Angaben sind möglich: **Typ** / **Beschreibung** **text** – Die Darstellung des Elements erfolgt durch Text. **image** – Die Darstellung des Elements erfolgt durch eine Grafik.
<view><value>	Mit dieser Option ist der Wert für den zuvor gewählten Typen festzulegen. **Typ** / **Wert** **text** – Angabe des Textes, der auf der zugehörigen Schaltfläche der Werkzeugleiste angezeigt werden soll. **image** – Angabe des voll qualifizierten Pfades zur Grafikdatei, die auf der zugehörigen Schaltfläche der Werkzeugleiste angezeigt werden soll. Unterstützte Typen sind '.gif' und '.jpg'.

<action><value>	Hier ist der Pfad zum Makro anzugeben, unter dem dieses in der JProtector Datenbasis gespeichert wurde, wie der nachfolgenden Abbildung zu entnehmen ist:  Die Pfadangabe muss alle Oberverzeichnisse mit Ausnahme der Wurzelverzeichnissesn 'Macros' enthalten. Als Pfadtrennzeichen ist der Schrägstrich '/' zu verwenden, im verwendeten Beispiel also 'CICS/BHAD'.

Ohio

Elemente vom Typ 'ohio' können zur Ausführung eines kompilierten Ohio Applets vewendet werden.

Syntax

```
<item type="ohio">
  <view>
    <type>text</type>
    <value>SignonToTPX</value>
  </view>
  <action>
    <value>SignOnToTPX</value>
  </action>
</item>
```

Option	Beschreibung
<view><type>	Mit dieser Option ist festzulegen, auf welche Weise JProtector das Element in der Werkzeugleiste darstellen soll. Folgende Angaben sind möglich: **Typ** / **Beschreibung** **text** – Die Darstellung des Elements erfolgt durch Text. **image** – Die Darstellung des Elements erfolgt durch eine Grafik.
<view><value>	Mit dieser Option ist der Wert für den zuvor gewählten Typen festzulegen. **Typ** / **Wert** **text** – Angabe des Textes, der auf der zugehörigen Schaltfläche der Werkzeugleiste angezeigt werden soll.

	image	Angabe des voll qualifizierten Pfades zur Grafikdatei, die auf der zugehörigen Schaltfläche der Werkzeugleiste angezeigt werden soll. Unterstützte Typen sind '.gif' und '.jpg'.
<action><value>	Hier ist der Aliasname des Ohio Applets anzugeben, das ausgeführt werden soll, sobald der Anwender die entsprechende Schaltfläche in der Werkzeugleiste anklickt.	

Skript

Elemente vom Typ 'script' können zur Ausführung einer Skript-Datei verwendet werden.

Syntax

```
<item type="script">
  <view>
    <type>image</type>
    <value>j:\jprot\skippy.jpg</value>
  </view>
  <action>
    <value>j:\jprot\cics.js</value>
    <call-parms>BKIP;YES</call-parms>
  </action>
</item>
```

Option	Beschreibung
<view><type>	Mit dieser Option ist festzulegen, auf welche Weise JProtector das Element in der Werkzeugleiste darstellen soll. Folgende Angaben sind möglich: **Typ** / **Beschreibung** **text** – Die Darstellung des Elements erfolgt durch Text. **image** – Die Darstellung des Elements erfolgt durch eine Grafik.
<view><value>	Mit dieser Option ist der Wert für den zuvor gewählten Typen festzulegen. **Typ** / **Wert** **text** – Angabe des Textes, der auf der zugehörigen Schaltfläche der Werkzeugleiste angezeigt werden soll. **image** – Angabe des voll qualifizierten Pfades zur Grafikdatei, die auf der zugehörigen Schaltfläche der Werkzeugleiste angezeigt werden soll. Unterstützte Typen sind '.gif' und '.jpg'.
<action><value>	Hier ist der voll qualifizierte Name der auszuführenden Skript-Datei anzugeben. Weitere Informationen zur Unterstützung und Ausführung von Skripts unter JProtector können Kapitel 'Skripts' auf Seite 91 entnommen werden.
<action><call-parms>	Mit dieser Option kann eine Argumentliste festgelegt werden, die an das auszuführende Skript zur Auswertung übergeben werden soll. Falls mehrere

	Argumente übergeben werden sollen, sind diese jeweils durch ein Semikolon ';' getrennt anzugeben.

Kapitel

17

Drucker

Beginnend mit JProtector Version 4 wurde das Drucken komplett überarbeitet. Dies liegt daran, dass mit Einführung der Java Laufzeitumgebung 1.4 erweiterte und verbesserte Schnittstellen für das Drucken zur Verfügung stehen.

Drucker werden nun, vergleichbar mit Tastaturbelegungen oder Farbschemata, im Rahmen einer eigenen Verwaltung definiert und können dann beliebigen Sessions zugeordnet werden.

Die Auswahl eines Druckers für die Verwendung in einer Session kann entweder über den Dialog zur Verwaltung der Sessionparameter erfolgen oder über das Druckermenü, das, wie nachfolgend abgebildet, eine Auflistung der definierten Drucker enthält:

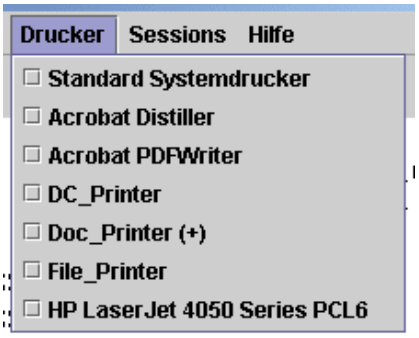


Abb. 82: Druckermenü

Der aktuell in den Sessionparametern ausgewählte Drucker ist mit einem '(+)' Zeichen versehen. Durch Markieren des entsprechenden Auswahlkästchens vor dem Druckernamen kann der gewünschte Drucker der aktiven Session zugeordnet und eine Verbindung aufgebaut (Selektion) bzw. abgebaut (Deselektion) werden.

Durch Aktivierung der auf Seite 35 beschriebenen Option zur automatischen Erkennung der installierten Drucker beim Start von JProtector kann erreicht werden, dass das abgebildete Druckermenü immer aktuell bzgl. der auf der Workstation verfügbaren Drucker ist.

Die allgemeine Verwaltung von Druckern erfolgt mit dem folgenden Dialog, der durch Auswahl des Menüpunktes 'Verwaltung::Drucker' eingeblendet wird.

Der Verwaltungsdialog

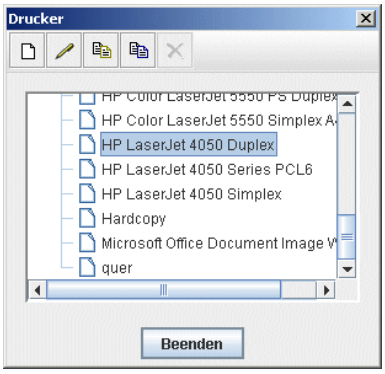


Abb. 83: Verwaltung der Drucker

Neu

Mit dieser Schaltfläche kann ein neuer Drucker erstellt werden.

Bearbeiten

Um den ausgewählten Drucker zu bearbeiten, ist diese Schaltfläche auszuwählen oder in der Baumansicht ein Doppelklick auf dem gewünschten Eintrag auszuführen.

Umbenennen

Diese Schaltfläche dient zum Umbenennen des in der Baumansicht markierten Druckers.

Kopieren

Unter Verwendung dieser Schaltfläche kann eine Kopie des markierten Druckers erstellt werden.

Löschen

Zum Löschen eines Druckers ist dieser in der Baumansicht zu selektieren und diese Schaltfläche auszuwählen. Der Versuch, einen Drucker zu löschen, der in mindestens einer Session verwendet wird, wird von JProtector abgewiesen.

Druckertypen

JProtector ermöglicht die Definition dreier verschiedener Druckertypen, die nachfolgend kurz beschrieben sind.

Gerätekontext Drucker

Ein Gerätekontext Drucker kann als bildschirmorientierter Drucker verstanden werden. Prinzipiell bildet dieser Druckertyp die Möglichkeiten eines Bildschirms ab, weswegen sich dieser Druckertyp in erster Linie zum Erstellen von Hardcopies eignet. Der Umfang der erzeugten Druckdatenmenge ist relativ groß. Dieser Umstand spielt jedoch beim Drucken von einseitigen Screenshots keine besondere Rolle.

Datei Drucker

Ein Datei Drucker kann für die Umleitung von Druckausgaben in Dateien verwendet werden. Die Einsatzmöglichkeiten hierfür sind vielfältig. So können z. B. auf dem Host gespeicherte Dokumente, die nur gedruckt werden können, mit Hilfe dieses Druckertyps in Dateien auf einer Workstation kopiert werden.

Dokumententyp Drucker

Dieser Druckertyp stellt mit Abstand die komplexesten Konfigurationsmöglichkeiten zur Verfügung, da er einen physikalischen Drucker abbildet und auch dessen Möglichkeiten zum Drucken verwendet. Mit Hilfe dieses Druckertyps können Dokumente für den Ausdruck mit druckerspezifischen Attributen versehen werden. Dies erfolgt z. B. unter Einbindung nativer PCL oder Postscript Kommandos in den Druckdatenstrom.

Der Druckerdialog

Zur Definition verschiedener Drucker steht der im Folgenden beschriebene Dialog zur Verfügung. Im oberen Bereich des Dialogs ist eine Auswahlliste enthalten, die die Selektion des gewünschten Druckertyps erlaubt. Der Inhalt des Dialogs ist vom gewählten Druckertyp abhängig. Bei der Neuanlage einer Druckerdefinition ist zunächst der Typ 'Gerätekontext Drucker' selektiert.

Gerätekontext Drucker

Die Definition der verschiedenen Druckeroptionen erfolgt über den nachfolgend abgebildeten Dialog.

Allgemein

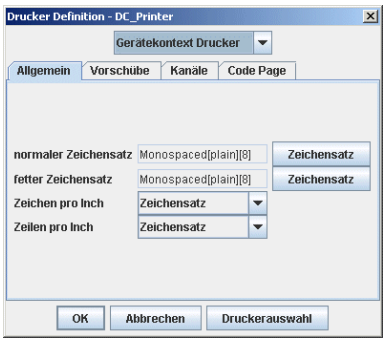


Abb. 84: Gerätekontext Drucker - Allgemein

normaler Zeichensatz

Dieses Feld zeigt die Wahl des Zeichensatzes für den Ausdruck normaler Daten. Die Veränderung des eingestellten Zeichensatzes erfolgt mit Hilfe eines Dialogs, der nach Auswahl der Schaltfläche 'Zeichensatz' eingeblendet wird.

fetter Zeichensatz

Der hier gewählte Zeichensatz wird bei Hardcopies für den Ausdruck von Daten verwendet, die mit dem Attribut 'high intensity' versehen sind. Der gewünschte Zeichensatz kann nach Auswahl der Schaltfläche 'Zeichensatz' im daraufhin eingeblendeten Dialog eingestellt werden.

Zeichen pro Inch

Eine vom gewählten Zeichensatz abweichende Angabe der Anzahl horizontal gedruckter Zeichen pro Inch (2,53 cm) kann durch eine Auswahl aus dieser Liste erreicht werden.

Zeilen pro Inch

Eine vom gewählten Zeichensatz abweichende Angabe der Anzahl vertikal gedruckter Zeilen pro Inch (2,53 cm) kann durch eine Auswahl aus dieser Liste erreicht werden.

Vorschübe

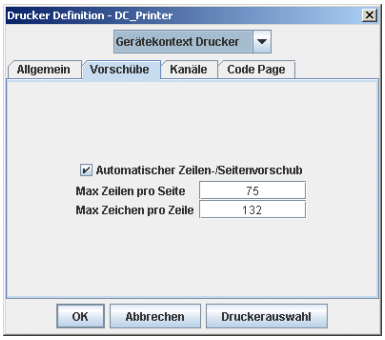


Abb. 85: Gerätekontext Drucker - Vorschübe

Max Zeilen pro Seite

Durch eine Eingabe in dieses Feld kann die maximale Anzahl der gedruckten Zeilen pro Seite festgelegt werden.

Max Zeichen pro Zeile

Durch eine Eingabe in dieses Feld kann die maximale Anzahl der gedruckten Zeichen pro Zeile festgelegt werden.

Automatischer Zeilen-/Seitenvorschub

Durch Auswahl dieser Kontrolloption wird erreicht, dass Zeilen- bzw. Seitenvorschübe automatisch von JProtector eingefügt werden.

Kanäle

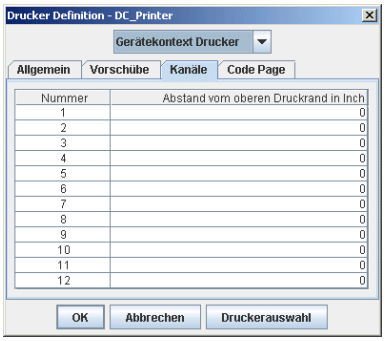


Abb. 86: Gerätekontext Drucker – Kanäle

Das SCS-Drucker Protokoll lässt den Zeilenvorschub auf einen bestimmten Kanal zu. Um dies nachzubilden, kann im abgebildeten Dialog eine Zuordnung zwischen Kanalnummer und Abstand vom oberen Druckrand in Inch erfolgen. Sollte der SCS-Druckdatenstrom den Vorschub auf einen bestimmten Kanal enthalten, positioniert JProtector die vertikale Ausgabeposition auf den zugewiesenen Wert. Bei fehlender Angabe wird lediglich ein Zeilenvorschub durchgeführt.

Die Eingabe einer Position kann nach einem Doppel-Mausklick in das entsprechende Tabellenfeld erfolgen, wodurch dieses in den Editiermodus versetzt wird.

Code Page

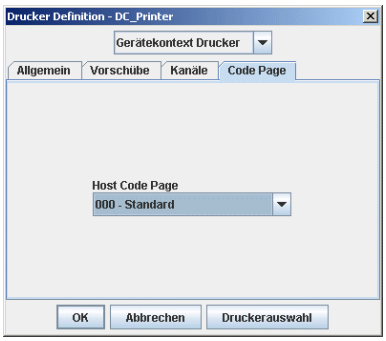


Abb. 87: Gerätekontext Drucker – Code Page

Host Code Page

Mit diesem Kombinationsfeld kann eine Host Code Page festgelegt werden, die zur Übersetzung der Druckdaten von EBCDIC nach Unicode verwendet werden soll. Bei keiner Angabe ('000 – Standard') wird die Host Code Page der zugehörigen Emulationssession verwendet.

Druckerauswahl

Die Zuordnung eines Druckers erfolgt über die Schaltfläche 'Druckerauswahl' im unteren Bereich des Dialogs. Daraufhin wird ein Standard Druckerauswahl Dialog der Java VM eingeblendet, in dem neben der Druckerauswahl auch eine Reihe von druckerspezifischen Einstellungen vorgenommen werden kann. Dazu kommt der nachfolgend abgebildete Dialog zum Einsatz:

Allgemein

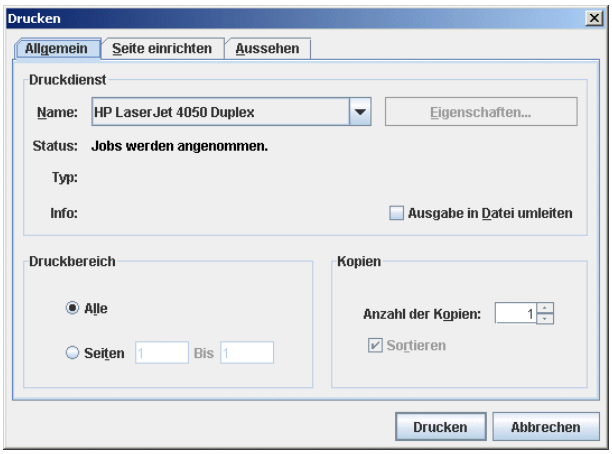


Abb. 88: Druckerauswahl - Allgemein

Mit dieser Dialogseite sind die allgemeinen Merkmale des Druckers festzulegen.

Seite einrichten

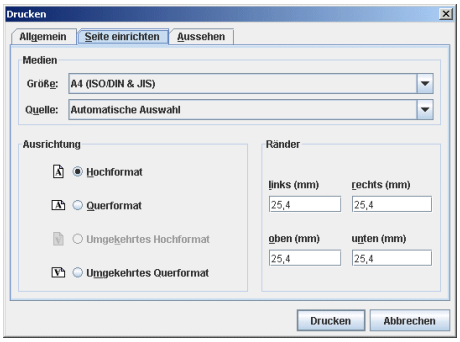


Abb. 89: Druckerauswahl – Seite einrichten

Mit dieser Dialogseite sind die seitenspezifischen Merkmale für den Ausdruck festzulegen.

Aussehen

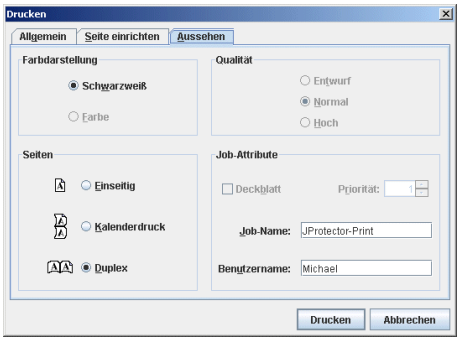


Abb. 90: Druckerauswahl - Aussehen

Mit dieser Dialogseite sind weitere Einstellungen zur Gestalt der Druckseite festzulegen.

Datei Drucker

Die Definition der verschiedenen Druckeroptionen erfolgt über den nachfolgend abgebildeten Dialog.

Allgemein

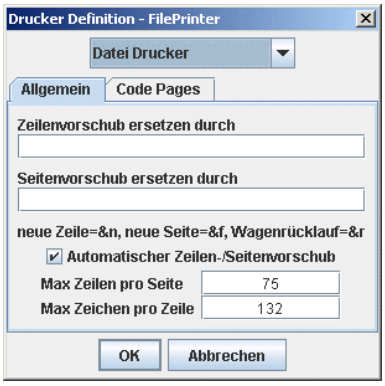


Abb. 91: Datei Drucker - Allgemein

Zeilenvorschub ersetzen durch

In diesem Feld kann ein Text eingegeben werden, der als Ersatz für ein Zeilenvorschubzeichen in die Datei gespeichert werden soll.

Seitenvorschub ersetzen durch

In diesem Feld kann ein Text eingegeben werden, der als Ersatz für ein Seitenvorschubzeichen in die Datei gespeichert werden soll.

Nachfolgend eine Liste der speziellen Ersatzzeichen:

&n Zeilenvorschub

&f Seitenvorschub

&r Wagenrücklauf

Max Zeilen pro Seite

Durch eine Eingabe in dieses Feld kann die maximale Anzahl der gedruckten Zeilen pro Seite festgelegt werden.

Max Zeichen pro Zeile

Durch eine Eingabe in dieses Feld kann die maximale Anzahl der gedruckten Zeichen pro Zeile festgelegt werden.

Automatischer Zeilen-/Seitenvorschub

Durch Auswahl dieser Kontrolloption wird erreicht, dass Zeilen- bzw. Seitenvorschübe automatisch von JProtector eingefügt werden.

Code Pages

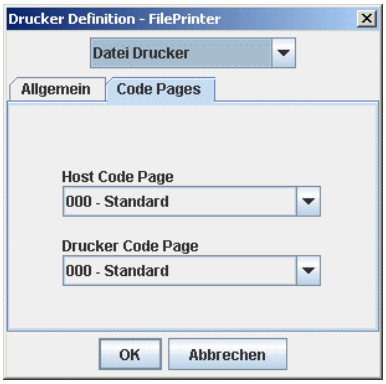


Abb. 92: Datei Drucker – Code Pages

Host Code Page

Mit diesem Kombinationsfeld kann eine Host Code Page festgelegt werden, die zur Übersetzung der Druckdaten von EBCDIC nach Unicode verwendet werden soll. Bei keiner Angabe ('000 – Standard') wird die Host Code Page der zugehörigen Emulationssession verwendet.

Drucker Code Page

Mit diesem Kombinationsfeld kann eine Code Page festgelegt werden, die zur Übersetzung der Druckdaten von Unicode nach ASCII/OEM/ANSI verwendet werden soll. Bei keiner Angabe ('000 – Standard') wird die voreingestellte Übersetzungstabelle der Java Virtual Machine verwendet.

Dokumententyp Drucker

Die Definition der verschiedenen Druckeroptionen erfolgt über den nachfolgend abgebildeten Dialog.

Vorspanndaten

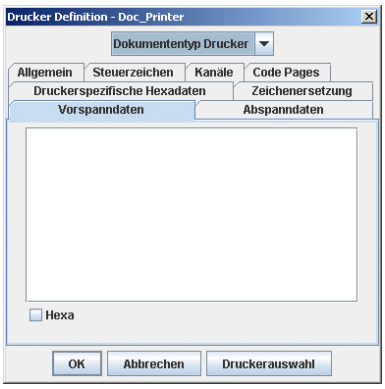


Abb. 93: Dokumententyp Drucker – Vorspanndaten

In diesem Editierfeld kann eine Sequenz von Daten eingegeben werden, die vor den eigentlichen Druckdaten an den Drucker gesendet werden soll. Mit einer Eingabe in dieses Feld ist es z. B. möglich, vor dem Ausdruck einen bestimmten Druckerzeichensatz zu aktivieren.

Sollten die eingegebenen Daten hexadezimales Format haben, ist dies durch Auswahl der Kontrolloption 'Hexa' anzuzeigen.

Abspanndaten

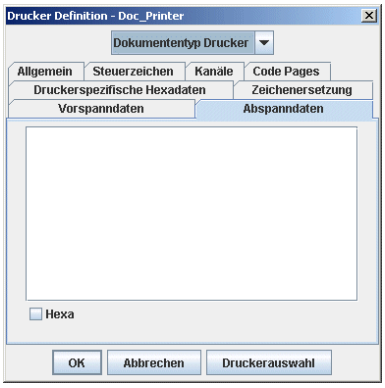


Abb. 94: Dokumententyp Drucker - Abspanndaten

In diesem Editierfeld kann, analog zu den Vorspanndaten, eine Sequenz von Daten eingegeben werden, die nach den eigentlichen Druckdaten an den Drucker gesendet werden soll. Mit einer Eingabe in dieses Feld ist es z. B. möglich, den Drucker in einen bestimmten Betriebszustand zu versetzen.

Sollten die eingegebenen Daten hexadezimales Format haben, ist dies durch Auswahl der Kontrolloption 'Hexa' anzuzeigen.

Druckerspezifische Hexadaten

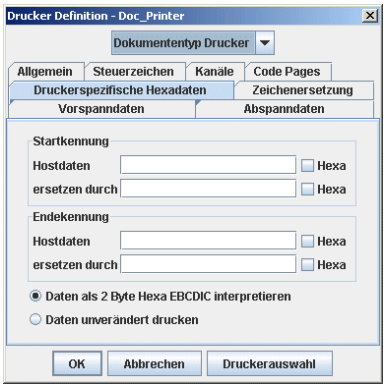


Abb. 95: Dokumententyp Drucker – Druckerspezifische Hexadaten

Es besteht die Möglichkeit, in die von einem Hostprogramm generierten Druckdaten hexadezimale Datenströme zur Druckersteuerung einzubinden. Beginn und Ende dieser Sequenzen sind durch spezielle Kennungen auszuzeichnen. Diese speziellen Datenströme wurden früher durch kleine Hardwareboxen, durch die der Druckdatenstrom geleitet wurde, erkannt und in entsprechende hexadezimale Zeichen umgesetzt.

Mit Hilfe dieses Dialogs können solche Datenströme bekannt gemacht werden. Dazu sind die Start- und Endekennung zu definieren, sowie die Zeichensequenz, durch die diese Kennungen ersetzt werden sollen. Weiterhin ist anzugeben, ob die angegebenen Sequenzen hexadezimale Eingabe darstellen.

Zum Zeitpunkt des Ausdrucks analysiert JProtector den Druckdatenstrom und ersetzt gegebenenfalls gefundene Start- und Endekennung durch die angegebenen Sequenzen.

Daten als 2 Byte Hexa EBCDIC interpretieren

Wenn dieses Auswahlfeld selektiert ist, interpretiert JProtector die druckerspezifischen Hexadaten als eine Sequenz von EBCDIC Daten in 2 Byte Character Darstellung. Diese Daten werden von JProtector vor der Verarbeitung nach ASCII übersetzt und anschließend zu einer Sequenz von echten Hexadaten zusammengefasst.

Daten unverändert drucken

Wenn dieses Auswahlfeld selektiert ist, verzichtet JProtector auf jede Interpretation der druckerspezifischen Hexadaten und übermittelt diese unverändert an den Drucker.

Zeichenersetzung

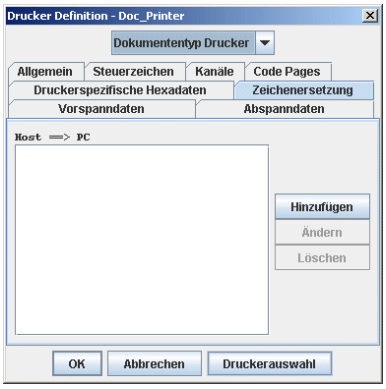


Abb. 96: Dokumententyp Drucker - Zeichenersetzung

Mit Hilfe dieses Dialogs können Zeichenersetzungen durchgeführt werden. Dazu ist die gewünschte Substitution in dem Dialog einzugeben, der nach Auswahl der Schaltfläche 'Hinzufügen' eingeblendet wird:

Abb. 97: Dokumententyp Drucker – Hostdaten Ersetzung

Die Hostdaten sowie die Ersatzzeichenkette sind zu definieren. Zusätzlich ist festzulegen, ob die jeweilige Angabe aus hexadezimalen Zeichen besteht.

Bereits definierte Substitutionen können im Zeichenersetzungsdialog durch Selektion in der Liste und anschließende Auswahl der Option 'Ändern' oder 'Löschen' bearbeitet oder entfernt werden.

JProtector führt während des Ausdrucks der Hostdaten eine Analyse durch und führt die gewünschte Substitution aus, falls die hier definierten Hostdaten gefunden werden.

Allgemein

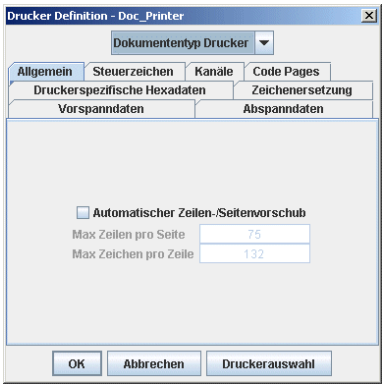


Abb. 98: Dokumententyp Drucker – Allgemein

Automatischer Zeilen-/Seitenvorschub

Durch Auswahl dieser Kontrolloption wird erreicht, dass Zeilen- bzw. Seitenvorschübe automatisch von JProtector eingefügt werden.

Max Zeilen pro Seite

Durch eine Eingabe in dieses Feld kann die maximale Anzahl der gedruckten Zeilen pro Seite festgelegt werden.

Max Zeichen pro Zeile

Durch eine Eingabe in dieses Feld kann die maximale Anzahl der gedruckten Zeichen pro Zeile festgelegt werden.

Steuerzeichen

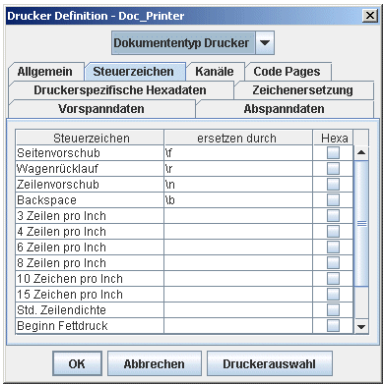


Abb. 99: Dokumententyp Drucker - Steuerzeichen

Mit Hilfe dieses Dialogs besteht die Möglichkeit, Ersatzzeichenketten für bestimmte Drucker Steuerzeichen zu definieren. Die festgelegten Ersetzungen werden von JProtector während des Ausdrucks im Druckdatenstrom durchgeführt.

Die gewünschten Substitutionen sind in der Tabellenspalte mit der Überschrift 'ersetzen durch' zu definieren. Dazu ist das entsprechende Tabellenfeld durch einen Doppelklick mit der Maus in den Editiermodus zu versetzen. Anschließend kann der Ersatztext eingegeben werden. Zusätzlich ist in der letzten Spalte der Tabelle festzulegen, ob der Ersatztext von JProtector als hexadezimale Zeichenkette interpretiert werden soll.

Kanäle

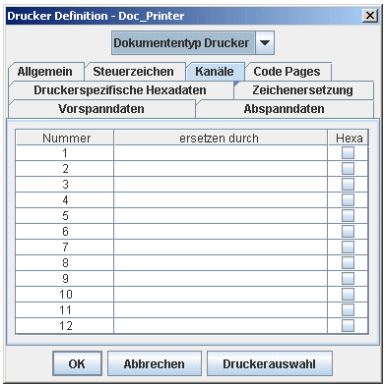


Abb. 100: Dokumententyp Drucker - Kanäle

Das SCS-Drucker Protokoll lässt den Zeilenvorschub auf einen bestimmten Kanal zu. Um dies nachzubilden, kann im abgebildeten Dialog festgelegt werden, durch welches Druckerkommando JProtector das Auftreten eines Vorschubs auf eine bestimmte Kanalnummer ersetzen soll.

Die Eingabe einer Ersatz Zeichenkette kann nach einem Doppel-Mausklick in das entsprechende Tabellenfeld erfolgen, wodurch dieses in den Editiermodus versetzt wird. Zusätzlich ist in der letzten Spalte der Tabelle festzulegen, ob der Ersatztext von JProtector als hexadezimale Zeichenkette interpretiert werden soll.

Code Pages

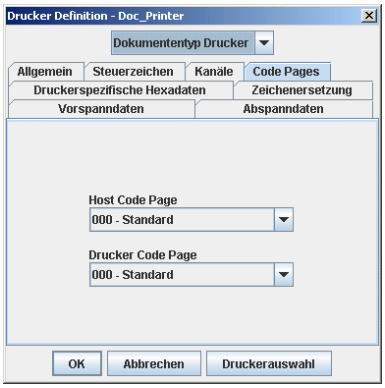


Abb. 101: Dokumententyp Drucker – Code Pages

Host Code Page

Mit diesem Kombinationsfeld kann eine Host Code Page festgelegt werden, die zur Übersetzung der Druckdaten von EBCDIC nach Unicode verwendet werden soll. Bei keiner Angabe ('000 – Standard') wird die Host Code Page der zugehörigen Emulationssession verwendet.

Drucker Code Page

Mit diesem Kombinationsfeld kann eine Code Page festgelegt werden, die zur Übersetzung der Druckdaten von Unicode nach ASCII/OEM/ANSI verwendet werden soll. Bei keiner Angabe ('000 – Standard') wird die voreingestellte Übersetzungstabelle der Java Virtual Machine verwendet.

Kapitel

18

Hostdrucker Gruppen

JProtector erlaubt die implizite Verbindung einer Hostdruckersession mit mehreren Terminalsessions. Damit kann gewährleistet werden, dass ein Benutzer immer eine Hostdruckersession zur Verfügung hat, solange eine der zugeordneten Terminalsessions geöffnet ist.

Die allgemeine Verwaltung von Hostdrucker Gruppen erfolgt mit dem folgenden Dialog, der durch Auswahl des Menüpunktes 'Verwaltung::Hostdrucker Gruppen' eingeblendet wird.

Der Verwaltungsdialog

Abb. 102: Verwaltung der Hostdrucker Gruppen

Neu

Mit dieser Schaltfläche kann eine neue Hostdrucker Gruppe erstellt werden.

Bearbeiten

Um die ausgewählte Hostdrucker Gruppe zu bearbeiten, ist diese Schaltfläche auszuwählen oder in der Baumansicht ein Doppelklick auf dem gewünschten Eintrag auszuführen.

Umbenennen

Diese Schaltfläche dient zum Umbenennen der in der Baumansicht markierten Gruppe.

Löschen

Zum Löschen einer Hostdrucker Gruppe ist diese in der Baumansicht zu selektieren und diese Schaltfläche auszuwählen.

Hostdrucker

Die Erstellung bzw. Bearbeitung einer Hostdrucker Gruppe erfolgt mit Hilfe des nachfolgend abgebildeten Dialogs.

Abb. 103: Hostdrucker Gruppe –Hostdrucker

Virtueller Gerätename

Hier kann ein virtueller VTAM Gerätename angegeben werden, den der Hostdrucker erhalten soll. Dazu sind zunächst der Auswahlknopf zu selektieren und anschließend der gewünschte VTAM Gerätename festzulegen. Falls eine Angabe in diesem Feld erfolgt, kann keine Angabe für 'Fixe Session ID' erfolgen.

Fixe Session ID

Hier kann eine fixe Session ID festgelegt werden, die der Hostdrucker erhalten soll. Dazu ist zunächst der Auswahlknopf zu selektieren und anschließend die gewünschte ID in der Auswahlbox zu selektieren. Diese Option ist zu wählen, falls bei Verwendung sicherer Verbindungen mit XPSDaemon der virtuelle VTAM Gerätename für den Hostdrucker im Rahmen eines Logon-Exits vergeben wird. Falls eine Angabe in diesem Feld erfolgt, kann keine Angabe für 'Virtueller Gerätename' erfolgen.

Zugeordneter Drucker

Hier ist der Drucker auszuwählen, der für die Druckausgabe verwendet werden soll. Der gewünschte Drucker ist in der Auswahlbox, die alle definierten JProtector Drucker auflistet, zu selektieren.

Sessions

Die Verknüpfung von Terminalsessions mit dem definierten Gruppendrucker erfolgt mit Hilfe des nachfolgend abgebildeten Dialogs.

Abb. 104: Hostdrucker Gruppen - Sessions

Neu

Mit dieser Schaltfläche kann eine neue Session in die Gruppe aufgenommen werden. Nach Auswahl der Schaltfläche wird ein Dialog zur Sessionauswahl eingeblendet. Jede Session kann nur in maximal eine Hostdrucker Gruppe aufgenommen werden.

Löschen

Mit dieser Schaltfläche kann die gewählte Session aus der Gruppe gelöscht werden.

TCP/IP

Die Verknüpfung von Terminalsessions mit dem definierten Gruppendrucker erfolgt mit Hilfe des nachfolgend abgebildeten Dialogs.

Abb. 105: Hostdrucker Gruppen – TCP/IP

Hostname/Hostadresse(n.n.n.n)

An dieser Stelle ist die TCP/IP Adresse des Hosts anzugeben, auf dem XPSDaemon läuft, für den die gemeinsam genutzte Druckersession aktiv ist.

Portnummer

Angabe der Portnummer, die von XPSDaemon überwacht wird.

Kapitel

19

IND$ - Filetransfer

JProtector stellt zum Up- und Download von Hostdateien eine Schnittstelle zum IND$File Service verschiedener Hostsysteme zur Verfügung. Die Definition und Ausführung einzelner Filetransfers erfolgt durch Auswahl des Menüpunktes 'Datei::IND$ - Filetransfer'.

Profiles

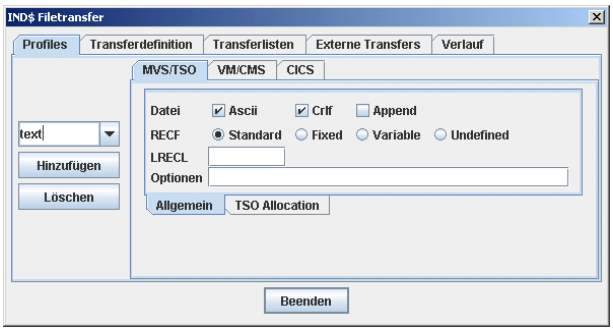


Abb. 106: IND$ Filetransfer - Profiles

Die Dialogseite 'Profiles' ist zur Definition verschiedener Transferprofiles für die unterschiedlichen Hostsysteme zu verwenden. Dabei beschreibt ein Profile die Parameter für einen Filetransfer.

Im linken Bereich der Dialogseite befindet sich ein aufklappbares Auswahlfeld, das eine Liste der verfügbaren Profiles zum ausgewählten Hostsystem - in der Abbildung 'MVS/TSO' - enthält. Durch Eingabe eines neuen Namens in das Editierfeld der Auswahlliste, und Drücken der Schaltfläche 'Hinzufügen', kann ein neues Profile für das aktive Hostsystem erstellt werden.

Im rechten Teil des Dialogs befinden sich verschiedene Unterseiten, die zur Festlegung der einzelnen Transferparameter dienen. Dabei stehen für die drei verfügbaren Hostsysteme 'MVS/TSO', 'VM/CMS' sowie 'CICS' (VSE) einzelne Unterseiten zur Verfügung. Die Unterseite für 'MVS/TSO' teilt sich zudem noch in 'Allgemein' und 'TSO Allocation'.

Eine Beschreibung der einzelnen Parameter entfällt an dieser Stelle. Für spezielle Fragen bzgl. der einzelnen Parameter sollte ein sachkundiger Mitarbeiter hinzugezogen werden.

Nachdem verschiedene Transferprofiles angelegt wurden, können mit Hilfe der Dialogseite 'Transferdefinition' einzelne Filetransfers definiert werden.

Transferdefinitionen

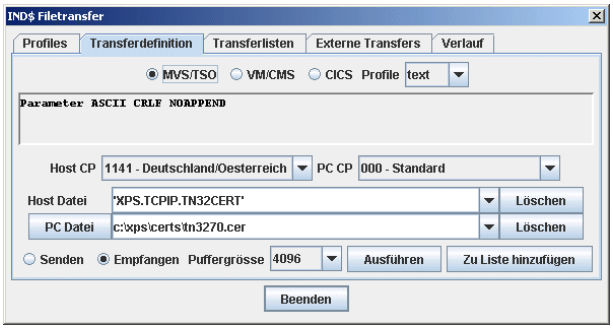


Abb. 107: IND$ Filetransfer - Transferdefinition

Auf dieser Dialogseite sind zunächst im oberen Bereich das gewünschte Hostsystem sowie das zu verwendende Profile auszuwählen. Das unterhalb liegende Textfeld zeigt die Parameter des gewählten Profiles an.

Im darunter liegenden Bereich kann für den Transfer sowohl eine spezielle Host Code Page als auch ein PC Code Page ausgewählt werden, die zur jeweiligen Übersetzung der Transferdaten herangezogen werden sollen, falls diese von den für die Emulationssession eingestellten Werten abweichen sollten.

Die Auswahl der Host- und PC Datei erfolgt über zwei Listen mit Editierfeld. Durch Drücken der Schaltfläche 'PC Datei' kann ein systemspezifischer Dialog eingeblendet werden, mit dessen Hilfe die PC Datei gewählt werden kann. Unter Verwendung der 'Löschen' Schaltflächen können die jeweils angezeigten Einträge aus den Listen gelöscht werden.

Des Weiteren ist die Art des Transfers festzulegen. Hier sind 'Senden' und 'Empfangen' verfügbar. Die jeweilige Transferrichtung ist clientseitig zu interpretieren. Sollte 'Senden' gewählt werden, überprüft JProtector, ob die gewählte PC Datei vorhanden ist.

Wenn eine Definition vollständig durchgeführt worden ist, kann der Transfer durch Auswahl der Schaltfläche 'Ausführen' gestartet werden.

Eine weitere Möglichkeit besteht darin, die Transferdefinition in eine Liste aufzunehmen. In einer Liste können beliebig viele Up- und Downloads für ein Hostsystem gespeichert werden. Die Verwendung von Listen bietet den Vorteil, dass mit einer Aktion sämtliche in der Liste definierten Transfers ausgeführt werden können. Diese Vorgehensweise ist bei Mehrfachtransfers, die häufiger ausgeführt werden, zu empfehlen. Nach Auswahl der Schaltfläche 'Zu Liste hinzufügen' wird das folgende Dialogfeld eingeblendet:

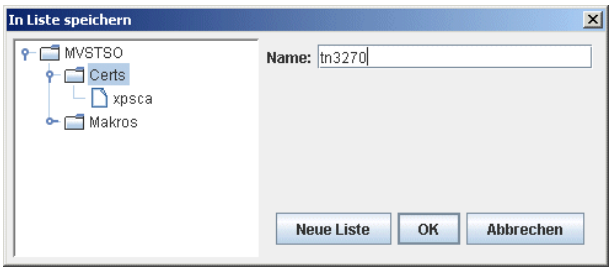


Abb. 108: Transfer in Liste speichern

Im linken Teil des Dialogs befindet sich eine Baumansicht, die alle Listen für das gewählte Hostsystem enthält. Durch Auswahl der Schaltfläche 'Neue Liste' kann eine neue Transferliste erstellt werden. Für das Speichern einer Transferdefinition in einer Liste ist die gewünschte Liste zunächst in der Baumansicht zu

selektieren, ein Name für den Transfer im Feld 'Name' einzugeben und die Schaltfläche 'OK' zu wählen. Die Transfernamen müssen innerhalb einer Liste eindeutig sein.

Transferlisten

Das Ausführen und Verwalten einzelner Transferlisten erfolgt mit Hilfe der Dialogseite 'Transferlisten'.

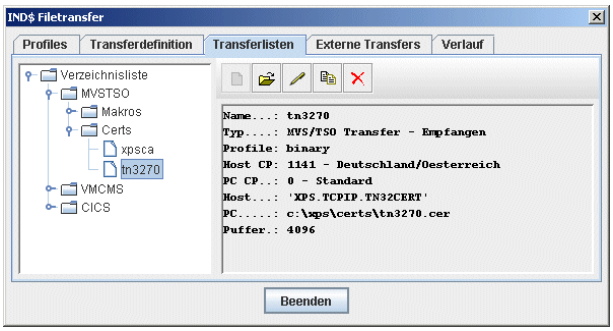


Abb. 109: IND$ Filetransfer - Transferlisten

Die Baumansicht enthält die verfügbaren Transferlisten, geordnet nach den verschiedenen Hostsystemen. Je nach ausgewähltem Knoten im Baum zeigt das Textfeld eine genauere Beschreibung der Auswahl an, und eine Untermenge der verfügbaren Aktionen ist auswählbar.

Neue Liste

Mit dieser Schaltfläche kann eine neue Transferliste für das gewählte System erstellt werden. Diese Schaltfläche ist nur aktiv, falls in der Baumansicht eines der Hostsysteme selektiert ist.

Filetransfer(s) ausführen

Durch Drücken dieser Schaltfläche wird der in der Baumansicht markierte Transfer ausgeführt. Falls in der Baumansicht eine Transferliste selektiert ist, werden alle darin definierten Transfers ausgeführt.

Bearbeiten

Um Veränderungen an einem Transfereintrag in einer Liste vorzunehmen, ist der gewünschte Transfer in der Baumansicht zu selektieren und diese Schaltfläche zu drücken. Im daraufhin eingeblendeten Dialog können die einzelnen Parameter für den Transfer verändert werden.

Umbenennen

Mit dieser Schaltfläche kann der in der Baumansicht selektierte Eintrag - Transfer oder Transferliste - umbenannt werden.

Löschen

Diese Schaltfläche dient zum Löschen des in der Baumansicht markierten Eintrages, sofern es sich dabei um einen Transfer oder eine Transferliste handelt.

Externe Transfers

Wie bereits bei der Beschreibung des JProtector Startup Parameters `'FILETRANSFER_DIR'` auf Seite 21 erwähnt, erlaubt JProtector die Ausführung extern definierter Filetransfers. Dazu sind Textdateien zu erstellen, die die entsprechenden Filetransfer Definitionen enthalten.

Sollte der Startup Parameter `'FILETRANSFER_DIR'` gesetzt worden sein, enthält der JProtector Filetransfer Dialog die nachfolgend abgebildete Seite:

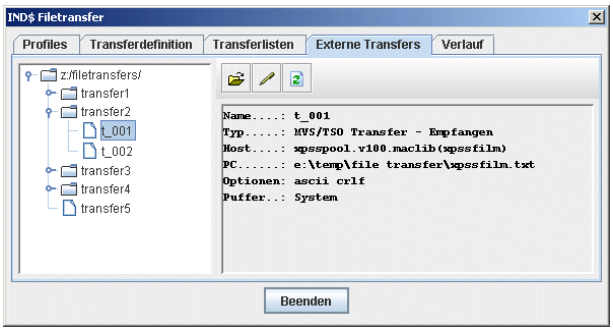


Abb. 110: IND$ Filetransfer – Externe Transfers

JProtector durchsucht das angegebene Verzeichnis für externe Filetransferdefinitionen und erstellt die Baumansicht. Sollte eine Datei mehr als eine Transferdefinition enthalten, wird für diese Datei ein Knoten in die Baumansicht eingefügt und die einzelnen darin enthaltenen Transfers als Elemente mit generierten Namen angezeigt.

Filetransfer(s) ausführen

Durch Drücken dieser Schaltfläche wird der in der Baumansicht markierte Eintrag ausgeführt. Dies können sowohl ein einzelner Transfer als auch alle Transfers in einer Textdatei sein.

Bearbeiten

Um Veränderungen an einem Transfereintrag in einer Liste vorzunehmen, ist der gewünschte Transfer in der Baumansicht zu selektieren und diese Schaltfläche zu drücken. Daraufhin wird der nachfolgend abgebildete Editor eingeblendet:

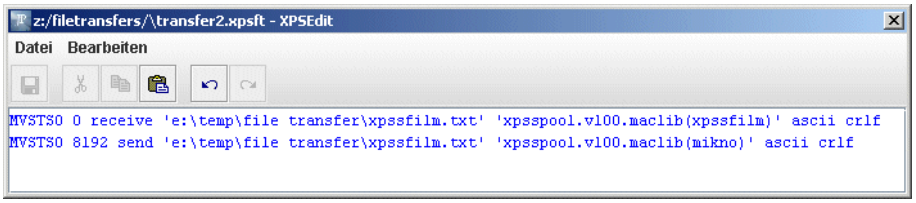


Abb. 111: IND$ Filetransfer – Bearbeitung externer Transferdefinitionen

Beschreibung des Formats einer externen Transferdefinition

Jede Definition muss sich in einer separaten Zeile befinden und mit einer Angabe für das Zielsystem beginnen. Mögliche Werte sind 'CICS', 'MVSTSO' und 'VMCMS'.

Daran schließt sich die gewünschte Puffergröße in Bytes an. Wenn ein Transfer mit der vom System vorgegebenen Puffergröße durchgeführt werden soll, dann ist dies durch eine Angabe von '0' anzuzeigen.

Anschließend erfolgt die Angabe der Transferrichtung. Zulässige Werte sind 'receive' und 'send'. Die Transferrichtung bezieht sich jeweils auf den Rechner, auf dem JProtector ausgeführt wird.

Daran schließt sich die Angabe der PC- bzw. Workstation Datei, die als Sendquelle ('send') oder als Empfangsziel ('receive') dienen soll, gefolgt von der entsprechenden Hostdatei. Beide Angaben sind in Hochkommata einzuschließen.

Den Abschluss einer Transferdefinition bildet eine Folge der gewünschten Transferoptionen. Die nachfolgende Tabelle zeigt eine Liste der zulässigen Transferoptionen:

	send	**receive**
CICS	ASCII, CRLF, BINARY	ASCII, CRLF, NOCRLF, BINARY
MVSTSO	ASCII, CRLF, APPEND, LRECL (n), RECFM (v|f|u), BLKSIZE (n), SPACE (n[,m]), AVBLOCK|TRACKS|CYLINDERS	ASCII, CRLF, APPEND
VMCMS	ASCII, CRLF, APPEND, LRECL n, RECFM v|f	ASCII, CRLF, APPEND

Nachladen

Durch Drücken dieser Schaltfläche werden die externen Filetransfer Definitionen nachgeladen. Damit können nachträglich durchgeführte Veränderungen im gewählten `'FILETRANSFER_DIR'` verfügbar gemacht werden.

Verlauf

Diese Dialogseite wird zur Anzeige des aktuellen Transferstatus bei der Ausführung von Filetransfers verwendet.

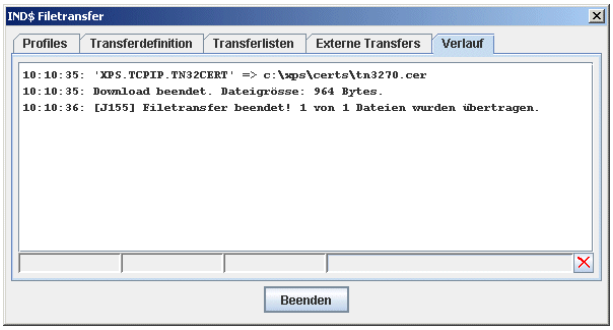


Abb. 112: IND$ Filetransfer - Verlauf

Mit Hilfe der Schaltfläche in der rechten unteren Ecke der Dialogseite kann die Verlaufsliste gelöscht werden. Während eines Filetransfers werden in der Statuszeile Informationen über den aktuellen Status, ('Datei 'i' von 'n'), die benötigte Zeit, sowie das übertragene Datenvolumen angezeigt. Bei einem Upload wird zusätzlich ein Verlaufsbalken eingeblendet, der visuell über den Status des Transferfortschritts informiert.

Kapitel

20

Maskendefinitionen

Diese Kapitel enthält die Beschreibung der Vorgehensweise zur Definition bestimmter Ausgabemasken zur Realisierung der Funktionen HotSpot und Single Signon.

JProtector speichert Maskendefinitionen in einer Textdatei im XML-Format ab. Name und Speicherort dieser Datei können mit der Option 'Datei mit Maskendefinitionen' auf der Karte 'Allgemein' der allgemeinen JProtector Einstellungen festgelegt werden.

Zur Vereinfachung der Administration kann die Datei mit den Maskendefinitionen auf einem zentralen Laufwerk abgelegt werden, so dass die Datei von mehreren Nutzern verwendet werden kann.

Maskendefinition

JProtector stellt einige Funktionen zur Verfügung, deren Ausführung nur für bestimmte Bildschirmmasken sinnvoll bzw. gewollt ist. Um dies zu ermöglichen ist es erforderlich, die entsprechenden Bildschirmmasken zu identifizieren.

Dies erfolgt im Rahmen einer Terminalsession durch Aktivierung der Funktion 'Maskendefinitionsmodus' aus dem 'Ansicht'-Menü. Wenn der Maskendefinitionsmodus aktiv ist, können zum einen neue Definitionen erstellt werden und zum anderen bereits bestehende Definitionen geändert werden.

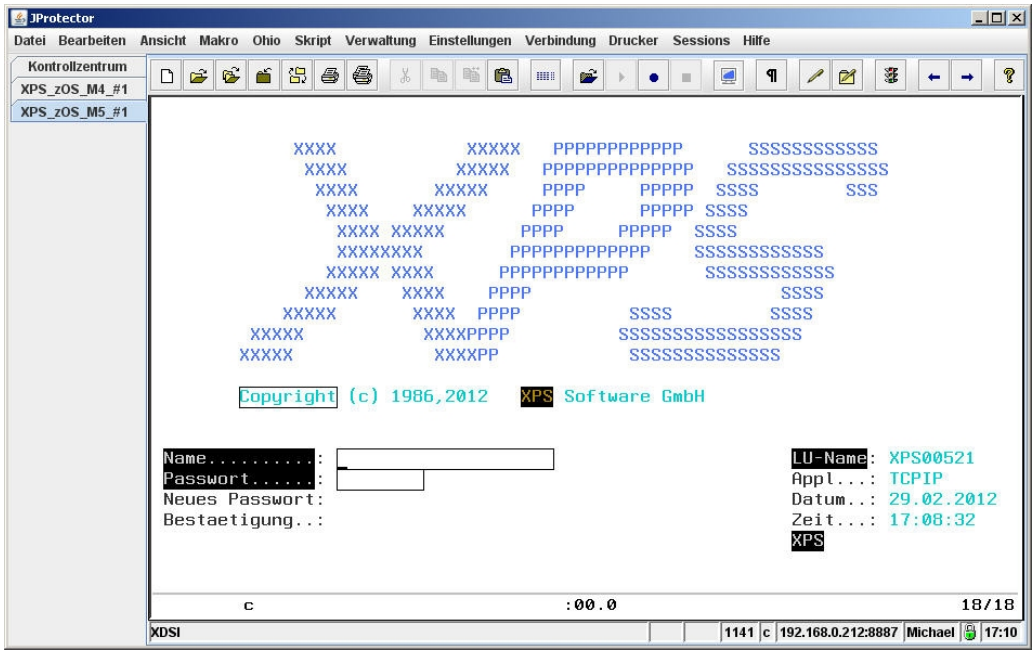


Abb. 113: Maskendefinitionsmodus

Die vorhergehende Abbildung zeigt das Emulationsfenster bei aktivem Maskendefinitionsmodus. Die angezeigte Bildschirmmaske ist eine XPSDaemon-Signon Maske.

Wie zu sehen ist, wurden fünf Bereiche zur Erkennung der Maske definiert. Dies sind die markierten (schwarz hinterlegten) festen Ausgabetexte der Maske. Diese Bereiche können vom Administrator frei gewählt werden. Es sind solche Bereiche zu wählen, die die Bildschirmmaske eindeutig identifizieren. Die Anzahl der Identifikationsbereiche ist prinzipiell beliebig.

Die drei umrahmten Bereiche zeigen an, dass diese Felder bereits mit speziellen Funktionen bzw. Attributen versehen wurden. In der abgebildeten Maske sind dies neben einem HotSpot die Eingabefelder für 'Name' und 'Passwort'. An Hand der Eingabefelder für Name und Passwort kann JProtector für diese Maske eine automatische Anmeldung für den Anwender durchführen.

Bildschirmmaske identifizieren

Zur Definition einer neuen Bildschirmmaske ist die Maske im Emulationsfenster anzuzeigen und der Maskendefinitionsmodus unter Verwendung des Menüpunktes 'Ansicht:Maskendefinitionsmodus' zu aktivieren, falls dies noch nicht der Fall sein sollte.

Anschließend sind, wie nachfolgend abgebildet, alle Bereiche der Maske unter Verwendung der Maus zu markieren, die zur eindeutigen Identifizierung der Maske herangezogen werden sollen:

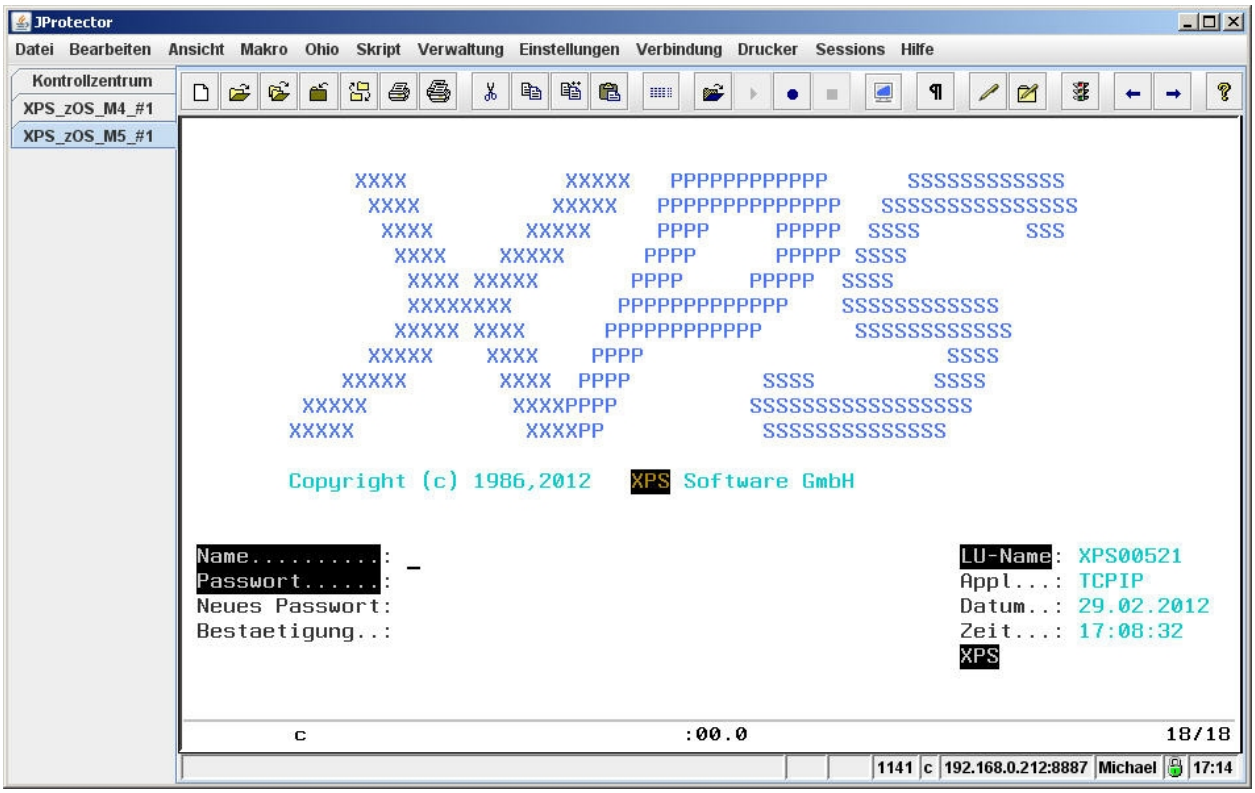


Abb. 114: Maske identifizieren

Nachdem alle Bereiche zur Identifizierung der Maske markiert sind, ist die Maske durch Auswahl der Schaltfläche ' ' aus der Werkzeugleiste bzw. durch Auswahl der Funktion 'Maske identifizieren' aus dem Popup-Menü für einen der markierten Bereich zu identifizieren.

Dazu ist im eigeblendeten Dialog ein eindeutiger Name für die identifizierte Maske festzulegen. Nach erfolgter Definition wird der vergebene Name im linken Bereich der Statusleiste des JProtector Fensters eingeblendet.

Definition von HotSpots

Sobald für eine Maske eine Definition angelegt wurde, können HotSpots für diese Maske definiert werden.

Unter einem HotSpot wird ein Bereich der Bildschirmmaske verstanden, der mit der Ausführung eines Ohio-Makros verknüpft ist. Der Anwender kann die Ausführung des Ohio-Makros durch einen Doppelklick mit der Maus auf den HotSpot veranlassen.

Zur Definition eines HotSpots ist eine bereits identifizierte Bildschirmmaske im Definitionsmodus anzuzeigen und der gewünscht HotSpot Bereich mit der Maus zu markieren. Anschließend ist unter Verwendung der rechten Maustaste ein Kontextmenü für den markierten HotSpot einzublenden, wie nachfolgend abgebildet:

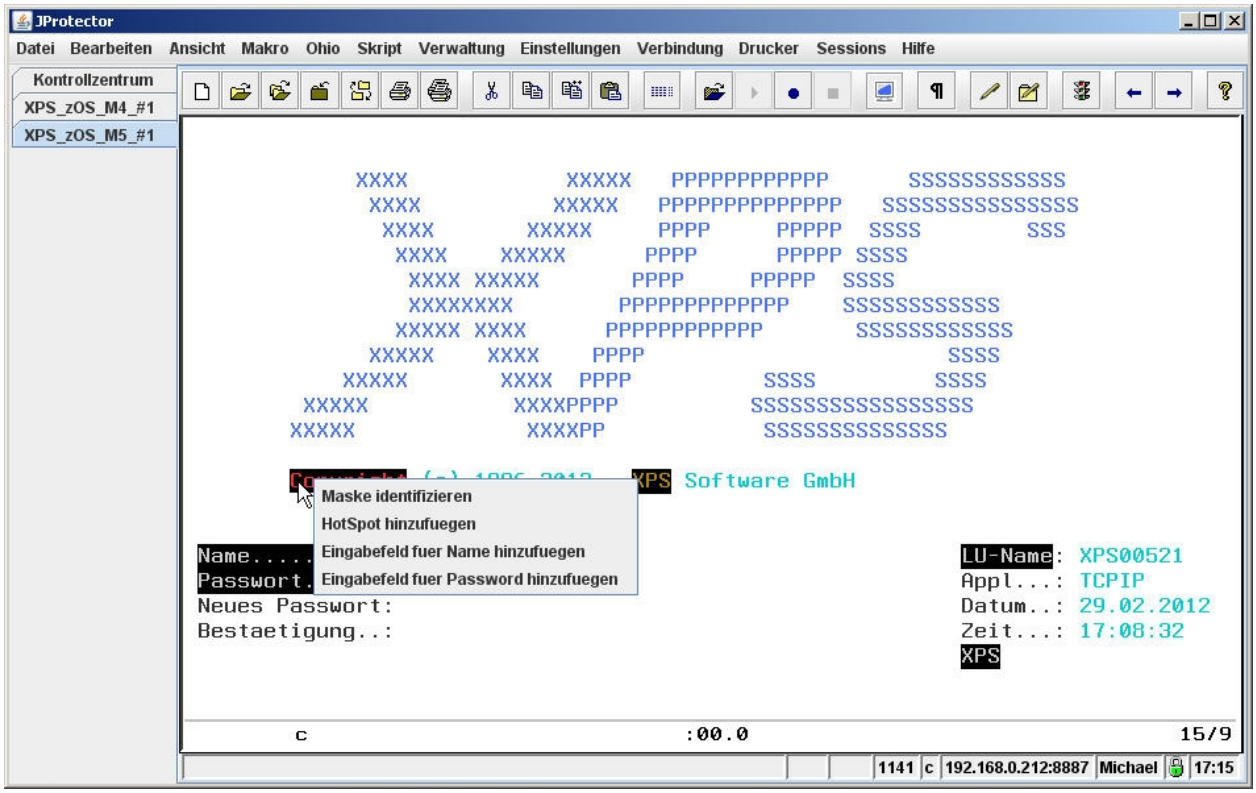


Abb. 115: HotSpot definieren

Aus dem eingeblendeten Kontextmenü ist die Funktion 'HotSpot hinzufügen' auszuwählen. Daraufhin wird ein Dialog eingeblendet, aus dem das zu verknüpfende Ohio-Makro für die Ausführung ausgewählt werden kann.

Nach erfolgter Zuordnung eines Ohio-Makros zum HotSpot wird die Bildschirmmaske wie folgt angezeigt:

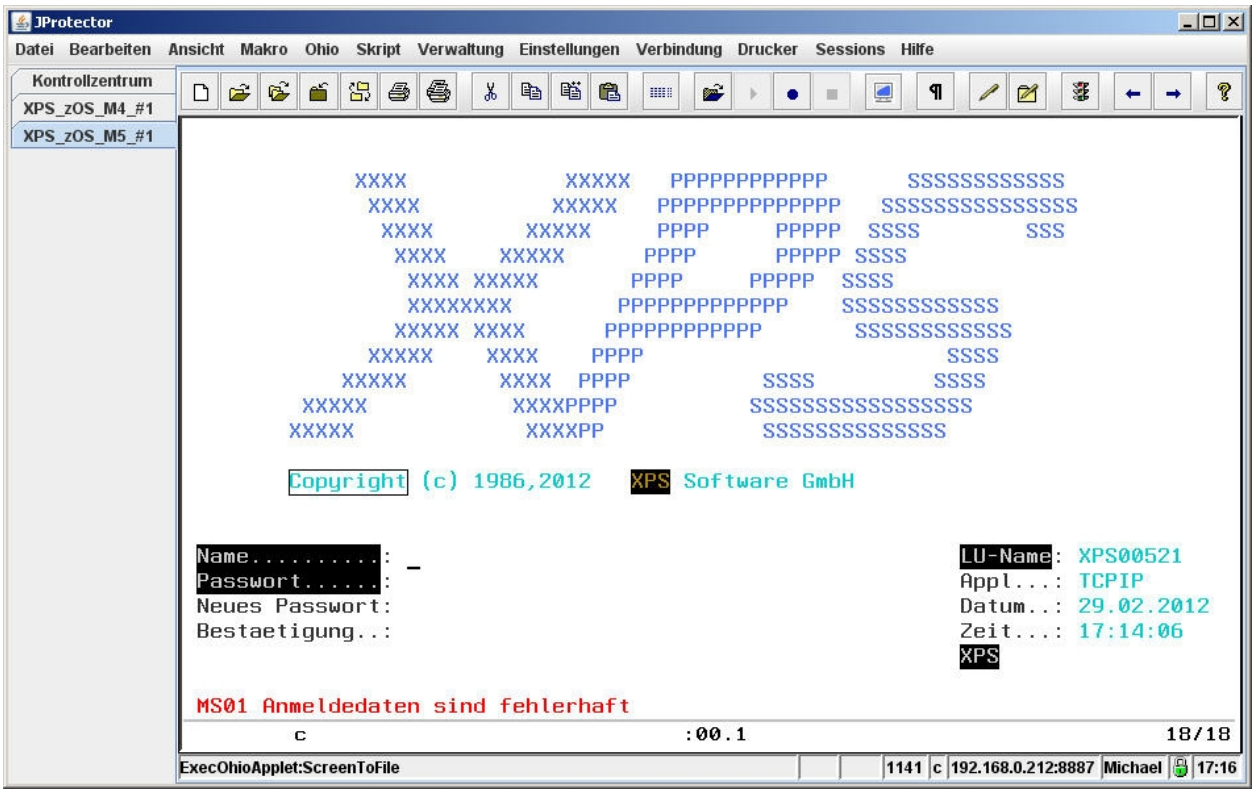


Abb. 116: HotSpot anzeigen

In der Abbildung wurde der Mauszeiger über dem HotSpot positioniert, was zur Anzeige des Namens des, dem HotSpot zugeordneten, Ohio-Makros im linken Bereich der Statuszeile der JProtector Fensters führt. Der HotSpot selbst wird mit einem Rahmen angezeigt.

Nach Beendigung des Definitionsmodus ändert sich die Bildschirmanzeige dahingehend, dass von den durchgeführten Definitionen lediglich noch der HotSpot-Rahmen sichtbar bleibt. Damit erhält der Anwender eine visuelle Information über die Bereiche, für die HotSpots definiert wurden.

Die HotSpot-Funktion kann nach erfolgter Definition durch einen Doppelklick mit der Maus in den festgelegten HotSpot-Bereich ausgeführt werden.

Single Signon

Eine weitere Möglichkeit für den Einsatz von Maskendefinitionen besteht in der Bereitstellung einer Single Signon Funktion für den Anwender.

Dazu sind zunächst alle Bildschirmmasken zu definieren, für die JProtector eine automatische Anmeldung des Benutzers durchführen soll.

Im Rahmen der Maskendefinition ist JProtector dann darüber zu informieren, welche Maskenbereiche für das Einspielen von Name und Passwort zu verwenden sind.

Dazu ist zunächst genauso vorzugehen, wie bei der Definition eines HotSpots. Allerdings ist im eingeblendeten Kontextmenü für einen markierten Bereich der Maske anstelle von 'HotSpot hinzufuegen' entweder 'Eingabefeld fuer Name hinzufuegen' oder 'Eingabefeld fuer Passwort hinzufuegen' auszuwählen, wie nachfolgend abgebildet.

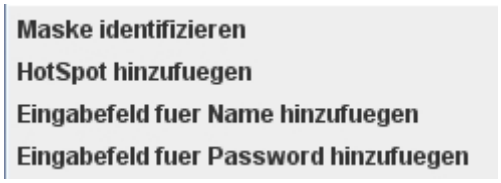


Abb. 117: Maskendefinition - Kontextmenü

Die nachfolgende Abbildung zeigt das Bildschirmfenster, nachdem Eingabefelder sowohl für den Namen als auch für das Passwort definiert wurden:

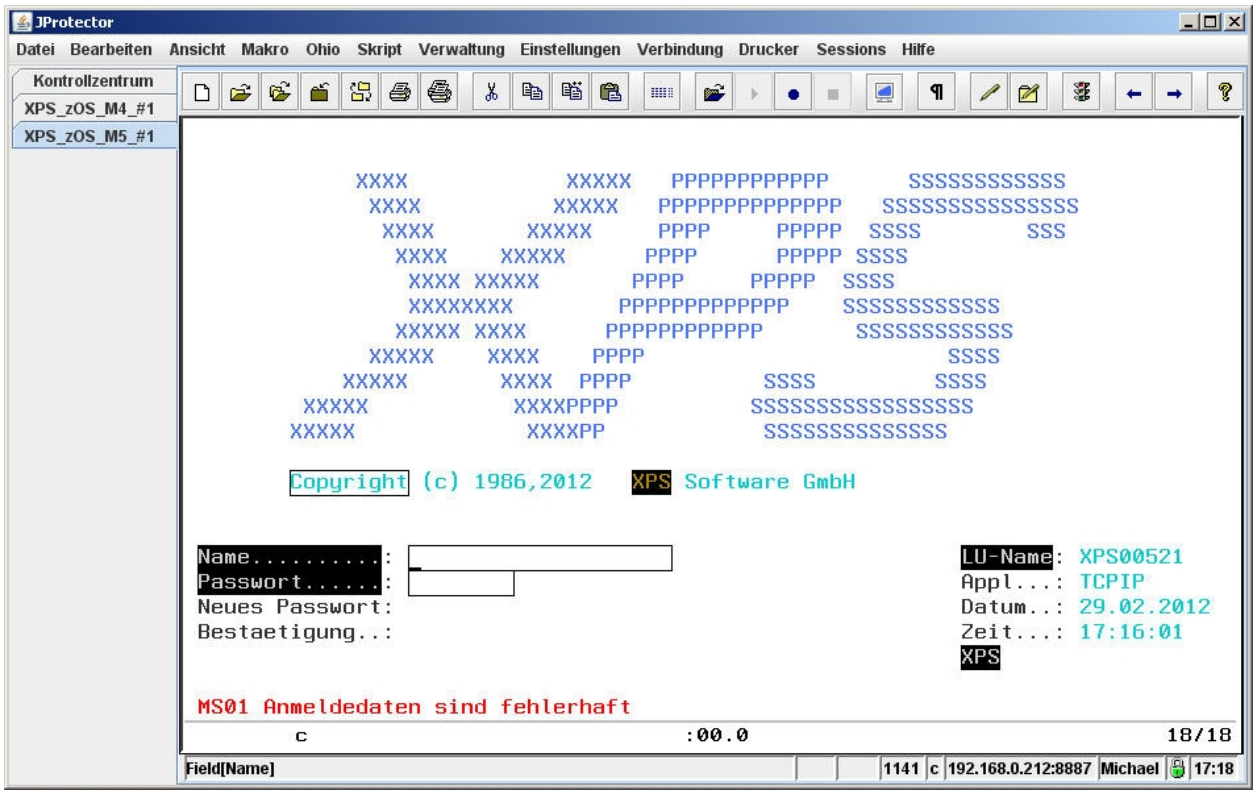


Abb. 118: Single Signon Definition

Wie in der Abbildung zu erkennen ist, werden die Felder für die Eingabe von Name und Passwort, ebenso wie der HotSpot, mit einer Umrahmung angezeigt.

Im Normalmodus zeigt JProtector die Umrahmung für definierte HotSpots weiterhin an, damit der Benutzer eine visuelle Rückmeldung über die definierten HotSpots hat. Die Eingabefelder für Name und Passwort werden nicht besonders gekennzeichnet.

Verwaltung

Unter dem Menüpunkt 'Verwaltung:Maskendefinitionen' stellt JProtector einen Dialog zur Verwaltung aller Maskendefinitionen zur Verfügung, die sich in der zugehörigen Definitionsdatei befinden. Die nachfolgende Abbildung zeigt den Verwaltungsdialog:

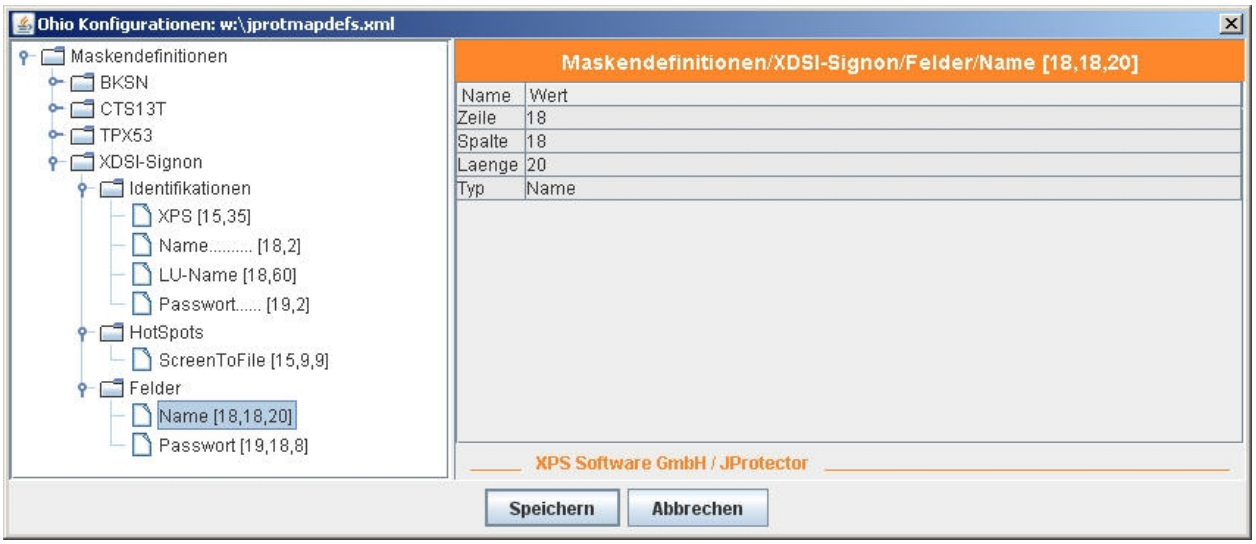


Abb. 119: Verwaltung der Maskendefinitionen

In der Baumansicht im linken Bereich der Anzeige sind alle Maskendefinitionen in aufsteigender alphabetischer Reihenfolge der vergebenen Namen aufgelistet.

Im rechten Bereich der Anzeige werden weitere Informationen für den jeweils in der Baumansicht selektierten Eintrag angezeigt.

Durch einen Klick mit der rechten Maustaste auf einen Eintrag in der Baumansicht wird ein Kontextmenü für den jeweils ausgewählten Eintrag eingeblendet, der das Löschen des Eintrags erlaubt. Beim Klick auf einen Maskennamen steht zusätzlich die Option 'Umbenennen' zur Verfügung.

Falls Veränderungen an den Definitionen vorgenommen werden, sind diese vor Verlassen des Dialogs durch Auswahl der Schaltfläche 'Speichern' in der aktiven Definitionsdatei zu sichern.

Kapitel

21

Sonstiges

Diese Kapitel enthält die Beschreibung einiger weiterer JProtector Funktionen.

Live Update

Das JProtector Programmpaket besteht aus dem Java Programmarchiv 'jprot.jar', das sich im Installationsverzeichnis befindet.

Um bei der Ausführung von JProtector als Applikation sicherzustellen, dass JProtector mit der aktuellen Programmversion arbeitet, und um die Versionsverwaltung möglichst einfach zu gestalten, enthält JProtector eine Live Update Funktion.

Dazu tauschen JProtector und XPSDaemon beim Programmstart die verwendete bzw. die erforderliche Versionsnummer des Programmarchivs aus. Sollte dabei festgestellt werden, dass ein Versionsabgleich notwendig ist, wird die veränderte Archivdatei vom Host auf den Clientrechner herunter geladen.

Eine Kopie der ersetzten Archivdatei wird im Unterverzeichnis 'Backup' zum Installationsverzeichnis abgespeichert.

Hinweis: Nach einem erfolgten Live Update muss JProtector neu gestartet werden, damit die neu geladene Archivdatei aktiv wird.

Systeminformation

Unter dem Menüpunkt 'Datei::Systeminformation' blendet JProtector einen Dialog ein, der eine Reihe aktueller Systeminformationen anzeigt. Im Einzelnen sind dies:

Informationen über den Benutzer

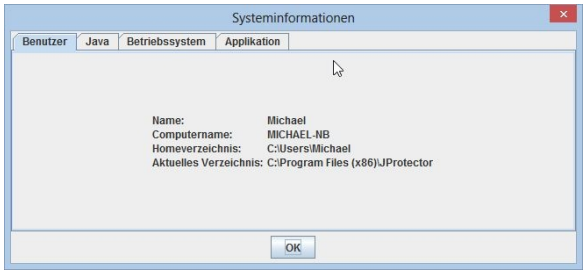


Abb. 120: Systeminformationen - Benutzer

Informationen über die verwendete Java Virtual Machine

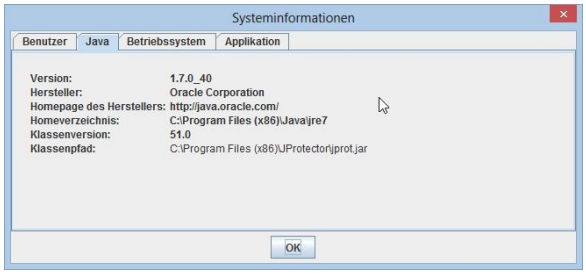


Abb. 121: Systeminformationen - Java

Informationen über das Betriebssystem

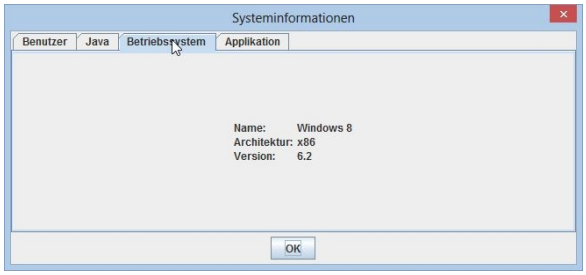


Abb. 122: Systeminformationen - Betriebssystem

Informationen über die Applikation

Abb. 123: Systeminformationen - Applikation

Helpdesk

Erstellung einer Secure Token Datei

JProtector erlaubt dem Administrator die Einschränkung des Funktionsumfangs für den Endanwender. Damit kann erreicht werden, dass z. B. bestimmte Einstellungen vom Endanwender nicht verändert werden dürfen.

Dies hat allerdings auch zur Folge, dass der JProtector Funktionsumfang für einen Administrator oder Helpdesk Mitarbeiter vor Ort beim Endanwender eingeschränkt ist.

Durch den Einsatz eines Secure Token ermöglicht JProtector die Freischaltung des gesamten Funktionsumfangs beim Endanwender durch einen autorisierten Mitarbeiter.

Dazu ist zunächst ein Secure Token zu generieren und in einer Datei abzuspeichern. Die Möglichkeit zur Generierung eines Secure Token wird durch Angabe des JProtector Startup Parameters

'<PARAM NAME="SECTOKEN_GENERATOR" VALUE="YES">', wie auf Seite 21 beschrieben, ermöglicht. Durch diese Angabe wird dem JProtector Verwaltungsmenü ein neuer Punkt hinzugefügt:

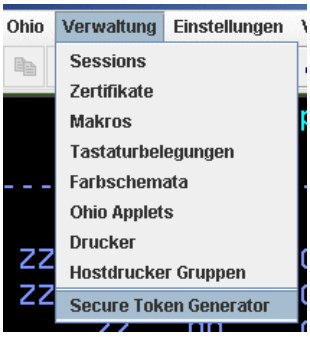


Abb. 124: Menüpunkt für den Secure Token Generator

Auswahl des Menüpunktes 'Secure Token Generator' führt zur Anzeige des folgenden Dialogs:

Abb. 125: Secure Token Generator

Der Secure Token Generator erstellt aus einer Konstanten und einem vom Administrator zu bestimmenden Passwort ein 16 stelliges Secure Token. Dazu ist nach der Eingabe des Passwortes samt Bestätigung die 'Generieren' Schaltfläche zu drücken.

Abschließend kann das Secure Token durch Auswahl der Schaltfläche 'Speichern' in eine vom Administrator zu bestimmende Datei abgespeichert werden.

Verwendung eines Secure Token

Damit der beschriebene Vorgang der Freischaltung des kompletten JProtector Funktionsumfangs erfolgen kann, ist der JProtector Startup Parameter '<PARAM NAME="HELPDESK_SECTOKEN_FILE" VALUE=[PFAD]>' für die Endanwender zu setzten. Die Pfadangabe muss exakt auf die gewünschte Secure Token Datei verweisen.

Durch diese Angabe fügt JProtector dem Hilfe Menü einen weiteren Eintrag hinzu:

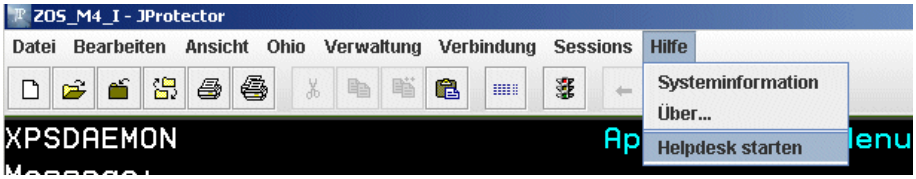


Abb. 126: Erweitertes Hilfemenü für den Helpdesk

Nach Auswahl des Menüpunktes 'Helpdesk starten' wird der folgende Dialog zur Eingabe des Passwortes für das entsprechende Secure Token eingeblendet:

Abb. 127: Eingabe des Passwortes für das Secure Token

In diesem Dialog ist das Passwort vom Helpdesk Mitarbeiter einzugeben. Sollte das Passwort korrekt sein, stellt JProtector sofort den gesamten Funktionsumfang bereit. Neben der Vervollständigung aller Menüs fügt JProtector zusätzlich einen neuen Eintrag in das Hilfe Menü ein, wie die nachfolgende Abbildung zeigt:

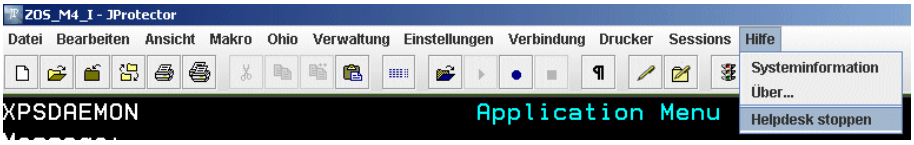


Abb. 128: Beenden des Helpdesks

Nachdem der Helpdesk Mitarbeiter die notwendigen Veränderungen vorgenommen hat, kann er durch Auswahl des Unterpunktes 'Helpdesk stoppen' aus dem Hilfe Menü den Helpdesk Modus wieder beenden. JProtector stellt daraufhin den ursprünglichen Funktionsumfang wieder her.

Kapitel

22

Nachrichten

J101 Beim Speichern der Datei trat ein Fehler auf.

Beschreibung: Bei der Speicherung von Daten auf der JProtector Datenbasis trat ein Fehler auf. Bei Auftreten dieser Nachricht ist es wahrscheinlich, dass die Datenbasis zerstört ist und nicht weiter verwendet werden kann.

Aktion: Der Systemadministrator ist über den Fehler zu informieren. Eine Kopie der fehlerhaften Datenbasis JProtector.xpsdb ist, falls möglich, zur Analyse an die XPS Software GmbH zu übersenden. Eventuell ist eine neue JProtector Datenbasis zu erstellen, indem die fehlerhafte zunächst umbenannt oder gelöscht wird. Beim Neustart von JProtector wird dann automatisch eine neue Datenbasis erzeugt.

J102 Die Angabe für mindestens eine benötigte Option fehlt.

Beschreibung: In einem Dialog wurde für mindestens eine Option keine Angabe gemacht, die JProtector für die weitere Verarbeitung zwingend braucht.

Aktion: Die benötigten Daten sind einzugeben oder die Dialogverarbeitung abzubrechen.

J103 Soll die Verbindung neu hergestellt werden?

Beschreibung: An den Sessioneinstellungen wurden Veränderungen vorgenommen, die erst nach einem erneuten Verbindungsaufbau zwischen JProtector und XPSDaemon aktiv werden.

Aktion: Falls gewünscht wird, dass die durchgeführten Veränderungen aktiv werden, ist die Verbindung durch Auswahl der Schaltfläche 'Ja' zu beenden und neu aufzubauen. Andernfalls kann auf einen sofortigen Neuaufbau der Verbindung verzichtet werden.

J104 Die ausgewählte Taste ist momentan nicht zugewiesen.

Beschreibung: Im unteren Bereich des Dialogs zur Tastenzuweisung wurde auf eine Hosttaste mit der Maus doppelgeklickt. Damit kann die momentane Zuordnung für die Hosttaste im oberen Bereich des Dialogs angezeigt werden. Die ausgewählte Hosttaste ist aktuell keiner Taste(nkombination) zugewiesen.

Aktion: Wenn die Hosttaste direkt durch eine Taste(nkombination) ausgelöst werden soll, ist eine Zuweisung durchzuführen. Die Vorgehensweise ist in Kapitel 'Tastenzuweisung – Hosttasten' auf Seite 79 beschrieben.

J105 Es wurde kein gültiges Clipboard Format gefunden.

Beschreibung: Die Zwischenablage des Systems enthält keine Daten, die von JProtector in die aktuelle Anwendungsmaske eingefügt werden können. Es besteht ausschließlich die Möglichkeit zum Einfügen von Text.

Aktion: Es ist keine weitere Aktion erforderlich. Wenn Daten aus einer anderen Applikation in das Emulationsfenster eingefügt werden sollen, sind die gewünschten Daten dort zunächst im Textformat in die Zwischenablage zu kopieren und anschließend in die Anwendungsmaske einzufügen.

J106 Momentan liegt keine Aufzeichnung vor.

Beschreibung: Es wurde der Versuch unternommen, ein Makro zu speichern oder abzuspielen. JProtector hat jedoch kein Makro im Zugriff, für das die Aktion ausgeführt werden könnte.

Aktion: JProtector kann durch Aufzeichnen oder Laden den Zugriff auf ein Makro erhalten, das dann gespeichert oder abgespielt werden kann. Die Vorgehensweisen zum Aufzeichnen und Laden sind im Kapitel 'Makros' auf Seite 67 beschrieben.

J107 Beim Laden/Erstellen der Datenbasis "JProtector.xpsdb" trat ein Fehler auf.

Beschreibung: JProtector kann die für die Verarbeitung benötigte Datenbasis JProtector.xpsdb nicht erstellen oder laden. Wenn dieser Fehler auftritt, ist entweder die verwendete Datenbasis zerstört, oder JProtector kann nicht in korrekter Weise auf das Dateisystem des Rechners zugreifen.

Aktion: Der Systemadministrator ist über den Fehler zu informieren. Eine Kopie der Datenbasis JProtector.xpsdb ist, falls möglich, an die XPS Software GmbH zur Analyse zu übersenden. Eventuell ist eine neue JProtector Datenbasis zu erstellen, indem die bemängelte zunächst umbenannt oder gelöscht wird. Beim Neustart von JProtector wird dann automatisch eine neue Datenbasis erzeugt.

J109 Das ausgewählte Makro wurde nicht gefunden

Beschreibung: Beim Versuch des Ladens eines Makros zur Ausführung trat ein Fehler auf. JProtector konnte das Makro auf der JProtector Datenbasis nicht mehr finden.

Aktion: Dieser Fehler sollte nicht auftreten, da JProtector Makrozuweisungen automatisch verwaltet, falls ein Makro gelöscht oder umbenannt wird. Bei Bedarf kann das Makro erneut aufgezeichnet und zugewiesen werden. Falls notwendig, ist eine neue Datenbasis zu erstellen, indem die existierende umbenannt oder gelöscht, und JProtector erneut gestartet wird.

J110 Das Umbenennen des ausgewählten Eintrages schlug fehl!

Beschreibung: Beim Umbenennen eines Eintrages auf der JProtector Datenbasis trat ein Fehler auf. Es besteht die Möglichkeit, dass die Datenbasis JProtector.xpsdb zerstört ist.

Aktion: Der Systemadministrator ist über den Fehler zu informieren. Eine Kopie der fehlerhaften Datenbasis JProtector.xpsdb ist, falls möglich, an die XPS Software GmbH zur Analyse zu übersenden. Eventuell ist eine neue JProtector Datenbasis zu erstellen, indem die fehlerhafte zunächst umbenannt oder gelöscht wird. Beim Neustart von JProtector wird dann automatisch eine neue Datenbasis erzeugt.

J111 Das Aufbauen der Verbindung zum Host schlug fehl!

Beschreibung: Beim Aufbauen einer TCP/IP Verbindung von JProtector zum TCP/IP Server von XPS, XPSDaemon, ist ein Fehler aufgetreten.

Aktion: Der Systemadministrator ist zu informieren, und es ist sicherzustellen, dass die Verbindung zu XPSDaemon hergestellt werden kann. Dazu ist zu prüfen, ob die in der Session definierte TCP/IP Adresse korrekt, und XPSDaemon auf dem Zielrechner gestartet ist und den ausgewählten Port überwacht.

J112 Fehler beim Lesen von Hostdaten.

Beschreibung: Beim Lesen von Daten über die TCP/IP Verbindung zwischen JProtector und XPSDaemon trat ein Fehler auf.

Aktion: Der Systemadministrator ist zu informieren, und es ist sicherzustellen, dass die Verbindung zu XPSDaemon hergestellt werden kann. Dazu ist zu prüfen, ob die in der Session definierte TCP/IP Adresse korrekt, und XPSDaemon auf dem Zielrechner gestartet ist und den ausgewählten Port überwacht.

J113 Fehler beim Schreiben von Hostdaten.

Beschreibung: Beim Schreiben von Daten über die TCP/IP Verbindung zwischen JProtector und XPSDaemon trat ein Fehler auf.

Aktion: Der Systemadministrator ist zu informieren, und es ist sicherzustellen, dass die Verbindung zu XPSDaemon hergestellt werden kann. Dazu ist zu prüfen, ob die in der Session definierte TCP/IP Adresse korrekt, und XPSDaemon auf dem Zielrechner gestartet ist und den ausgewählten Port überwacht.

J114 TRex meldet den folgenden Fehler:

Beschreibung: Im Zusammenhang mit der Datenübertragung über den TRex Tunnel ist ein Fehler aufgetreten, der mit dieser Nachricht näher beschrieben wird.

Aktion: Sollte der gemeldete Fehler nicht anwendungsbedingt sein, ist der Systemadministrator zu informieren.

J122 Session ist geöffnet!

Beschreibung: Es wurde versucht, eine momentan geöffnete Session zu verändern oder zu löschen. Dies ist nicht zulässig.

Aktion: Das Bearbeiten einer geöffneten Session erfolgt durch Auswahl des Menüpunktes Einstellungen::Session. Das Löschen einer geöffneten Session ist nicht möglich. Hierzu ist die Session zunächst zu beenden.

J125 Aufruf eines Makros in einem Makro ist nicht erlaubt!

Beschreibung: Der JProtector Makrorekorder erlaubt den Aufruf eines Makros aus einem anderen heraus nicht. Diese Nachricht erscheint, wenn z.B. beim Aufzeichnen eines Makros eine Taste(nkombination) gedrückt worden ist, die als Shortcut zur Ausführung eines anderen Makros verwendet wird.

Aktion: Es ist keine weitere Aktion notwendig. Bei Bedarf ist die Aufzeichnung des Makros zu wiederholen.

J126 Allgemeine Einstellungen werden gerade in einer anderen Session bearbeitet.

Beschreibung: JProtector erlaubt die Bearbeitung der allgemeinen Einstellungen nicht aus mehreren Sessions gleichzeitig, um die Integrität der Daten sicherzustellen.

Aktion: Die allgemeinen Einstellungen sind in der Session zu bearbeiten, in der der entsprechende Dialog bereits geöffnet ist.

J127 Aufruf eines Ohio Applets in einem Makro ist nicht erlaubt!

Beschreibung: Der JProtector Makrorekorder erlaubt den Aufruf eines Ohio Applets nicht aus einem Makro heraus. Diese Nachricht erscheint, wenn z.B. beim Aufzeichnen eines Makros eine Taste(nkombination) gedrückt worden ist, die als Shortcut zur Ausführung eines Ohio Applets verwendet wird.

Aktion: Es ist keine weitere Aktion notwendig. Bei Bedarf ist die Aufzeichnung des Makros zu wiederholen.

J129 Das gewählte TCP/IP Ziel ist momentan nicht erreichbar. Möchten Sie diese Einstellung übernehmen?

Beschreibung: Bei der Definition einer Session wurde ein TCP/IP Name für den Host ausgewählt. JProtector kann mit dieser TCP/IP Adresse momentan keine Verbindung aufbauen.

Aktion: Es ist sicherzustellen, dass ein gültiger TCP/IP Name ausgewählt wird. Eventuell ist der Systemadministrator zu Rate zu ziehen.

J130 Unbekannter Verbindungsfehler.

Beschreibung: Bei der Übertragung von Daten zwischen JProtector und XPSDaemon ist ein unbekannter Verbindungsfehler aufgetreten.

Aktion: Die Verbindung ist neu aufzubauen, indem die Session beendet und wieder gestartet wird. Sollte der Fehler wiederholt auftreten, ist der Systemadministrator darüber in Kenntnis zu setzen.

J131 HTTP-Header Lesefehler. Verbindung unterbrochen.

Beschreibung: JProtector konnte einen HTTP-Header nicht korrekt lesen.

Aktion: Die Datenübertragung funktioniert nicht korrekt. Die Session ist neu zu starten. Sollte der Fehler weiterhin auftreten, ist der Systemadministrator zu informieren.

J132 HTTP-Header Importfehler.

Beschreibung: JProtector konnte einen HTTP-Header nicht korrekt importieren.

Aktion: Die Datenübertragung funktioniert nicht korrekt. Die Session ist neu zu starten. Sollte der Fehler weiterhin auftreten, ist der Systemadministrator zu informieren.

J133 XPS-Header Lesefehler. Verbindung unterbrochen.

Beschreibung: Bei der Datenübertragung stellte JProtector einen Fehler im internen Datenbeschreibungspaket fest.

Aktion: Die Datenübertragung funktioniert nicht korrekt. Die Session ist neu zu starten. Sollte der Fehler weiterhin auftreten, ist der Systemadministrator zu informieren.

J134 Datenlesefehler. Verbindung unterbrochen.

Beschreibung: Beim Lesen von Daten über die TCP/IP-Verbindung trat ein Fehler auf.

Aktion: Die Datenübertragung funktioniert nicht korrekt. Die Session ist neu zu starten. Sollte der Fehler weiterhin auftreten, ist der Systemadministrator zu informieren.

J135 HTTP-Trailer Lesefehler. Verbindung unterbrochen.

Beschreibung: JProtector konnte einen HTTP-Trailer nicht korrekt lesen.

Aktion: Die Datenübertragung funktioniert nicht korrekt. Die Session ist neu zu starten. Sollte der Fehler weiterhin auftreten, ist der Systemadministrator zu informieren.

J137 Fehler bei der Verarbeitung des geheimen Schlüssels.

Beschreibung: Bei der Verarbeitung des geheimen Schlüssels, der zur Verschlüsselung des Datenaustauschs zwischen XPSDaemon und JProtector verwendet wird, trat ein Fehler auf. Die Sessionverarbeitung kann nicht weiter fortgesetzt werden.

Aktion: Zunächst ist ein erneuter Versuch des Verbindungsaufbaus zu unternehmen. Sollte der Fehler wiederum auftreten, ist der Systemadministrator zu informieren.

J138 Geheimer Schlüssel mit fehlerhafter Länge.

Beschreibung: Die Übertragung des geheimen Schlüssels zwischen XPSDaemon und JProtector konnte nicht erfolgreich durchgeführt werden. Die Sessionverarbeitung kann nicht weiter fortgesetzt werden.

Aktion: Zunächst ist ein erneuter Versuch des Verbindungsaufbaus zu unternehmen. Sollte der Fehler wiederum auftreten, ist der Systemadministrator zu informieren.

J139 Vom Host erhaltene Versionsupdateinfo ist fehlerhaft.

Beschreibung: Beim Verbindungsaufbau wurde festgestellt, dass ein Live Update der Archivdateien auf dem Clientrechner durchzuführen ist. Die daraufhin notwendige Übermittlung der benötigten Versionsinformationen ist fehlgeschlagen, so dass der Live Update nicht fehlerfrei durchgeführt werden kann.

Aktion: Zunächst ist ein erneuter Versuch des Verbindungsaufbaus zu unternehmen. Sollte der Fehler wiederum auftreten, ist der Systemadministrator zu informieren.

J140 Die Ausführung von JProtector wird nun beendet.

Beschreibung: Mit dieser Nachricht informiert JProtector den Benutzer darüber, dass nach einem abgelehnten Versionsupdate die Emulation die Verarbeitung nicht fortsetzen kann.

Aktion: Es ist keine weitere Aktion seitens des Anwenders notwendig.

J142 Zur Aktivierung der Änderungen ist ein Neustart von JProtector notwendig!

Beschreibung: Mit dieser Nachricht informiert JProtector den Benutzer darüber, dass nach einem erfolgten Live Update ein Neustart der Emulation notwendig ist.

Aktion: Zur Aktivierung der geladenen Änderungen ist JProtector neu zu starten.

J145 Der folgende Ausnahmefehler ist aufgetreten: ... Der Fehler wurde in der Datei ... protokolliert!

Beschreibung: Im Verlauf einer JProtector Session wurde von der ausführenden Java Virtual Machine der in der Nachricht beschriebene Ausnahmefehler abgefangen. Eine genauere Protokollierung des Fehlers erfolgte in die angegebene Datei im JProtector Verzeichnis.

Aktion: Abhängig vom aufgetretenen Ausnahmefehler ist zu entscheiden, ob die JProtector Session fortgesetzt werden soll, falls dies möglich ist. Der Systemadministrator ist über den aufgetretenen Fehler zu informieren und gegebenenfalls ist die Protokolldatei an die XPS Software GmbH zur Analyse zu übersenden.

X009 Ungültiger Benutzer

Beschreibung: Der von JProtector verschlüsselt an XPSDaemon übermittelte Benutzername kann nicht korrekt entschlüsselt werden. Die Emulationssession wird beendet.

Aktion: Der Systemadministrator ist über den Fehler zu informieren.

X011 Ungültiger Public Key

Beschreibung: Der von JProtector an XPSDaemon gesendete öffentliche Schlüssel entspricht nicht dem erwarteten Format. Die Emulationssession wird beendet.

Aktion: Der Systemadministrator ist über den Fehler zu informieren.

X012 Benutzer nicht definiert.

Beschreibung: JProtector ermittelt den Benutzernamen aus der Netzwerkanmeldung oder, falls zulässig, aus der Angabe für den Benutzernamen bei den allgemeinen Sessionparametern. Der ermittelte Name ist auf der XPSDaemon Benutzerdatei nicht definiert, so dass die Session nicht fortgesetzt werden kann.

Aktion: Der Systemadministrator ist über den Fehler zu informieren.

X015 Keine Instanzdaten für Benutzer.

Beschreibung: XPSDaemon ist es nicht möglich, die von JProtector gesendeten Daten einem Benutzer zuzuordnen. Die Fortsetzung der Session ist ausgeschlossen.

Aktion: Die Session ist erneut aufzubauen. Sollte die Fehlernachricht wiederholt erscheinen, ist der Systemadministrator zu informieren.

X018 Ändern des Druckernamens nicht erlaubt.

Beschreibung: Beim Aufbau einer Druckersession wurde festgestellt, dass der Benutzer einen LU/Pool Namen für den Drucker ausgewählt hat, jedoch hostseitig nicht dazu autorisiert wurde.

Aktion: Der LU/Pool Name ist aus der Sessiondefinition zu entfernen.

X019 Ungültige Sequenznummer.

Beschreibung: XPSDaemon hat eine ungültige Sequenznummer für diese Session ermittelt. Die Verwendung von Sequenznummern verhindert das Einspielen einer aufgezeichneten JProtector Session zu einem späteren Zeitpunkt. Die Session wird aus Sicherheitsgründen nicht weiter fortgesetzt.

Aktion: Der Systemadministrator ist über den Fehler zu informieren.

X020 TCP/IP Fehler.

Beschreibung: XPSDaemon hat einen TCP/IP Fehler erhalten.

Aktion: Die Session ist erneut aufzubauen. Sollte der Fehler weiterhin bestehen, ist der Systemadministrator zu informieren.

X024 Keine vertrauenswürdigen Aussteller vorhanden.

Beschreibung: Beim Aufbau einer Session sollte die Benutzerauthentisierung über ein X.509 Zertifikat erfolgen. In der XPSDaemon Systemumgebung sind jedoch keine digitalen Zertifikate vertrauenswürdiger Aussteller geladen. In diesem Fall ist die Verwendung von Zertifikaten nicht möglich.

Aktion: Wenn die Verwendung von Zertifikaten erforderlich ist, ist der Systemadministrator über diese Nachricht zu informieren.

X025 Ungültiges Zertifikat - kein vertrauenswürdiger Aussteller.

Beschreibung: Zur Benutzerauthentisierung wurde ein X.509 Zertifikat verwendet, dessen Aussteller in XPSDaemon nicht als vertrauenswürdig deklariert wurde. Dieses Zertifikat kann nicht zur Benutzerauthentisierung verwendet werden.

Aktion: Entweder ist auf die Verwendung des Zertifikates zu verzichten, oder der Systemadministrator ist darüber zu informieren, dass der Zertifikatsaussteller in der XPSDaemon Systemumgebung als vertrauenswürdig zu deklarieren ist.

X026 Ungültiges Zertifikat - Gültigkeitsdauer abgelaufen.

Beschreibung: Zur Benutzerauthentisierung wurde ein X.509 Zertifikat verwendet, das nicht mehr gültig ist. Dieses Zertifikat kann nicht zur Benutzerauthentisierung verwendet werden.

Aktion: XPSDaemon erlaubt die Benutzerauthentisierung nur über X.509 Zertifikate, deren Gültigkeitsdauer nicht abgelaufen ist. Es ist sicherzustellen, dass ein gültiges X.509 Zertifikat verwendet wird.

X027 Ungültiges Zertifikat - nicht unterstützter Algorithmus.

Beschreibung: Im ausgewählten Zertifikat kommt ein Algorithmus zum Einsatz, der von XPSDaemon nicht unterstützt wird. Dieses Zertifikat kann nicht zur Benutzerauthentisierung verwendet werden.

Aktion: Der Systemadministrator ist über diese Meldung zu informieren.

X028 Ungültiges Zertifikat - ungültige Signatur.

Beschreibung: Die im Zertifikat enthaltene digitale Signatur ist ungültig. Dieses Zertifikat kann nicht zur Benutzerauthentisierung verwendet werden.

Aktion: Es ist sicherzustellen, dass ein gültiges Zertifikat verwendet wird..

X029 Ungültiges Zertifikat - Zertifikat nicht unterstützt.

Beschreibung: Das Format des ausgewählten Zertifikats wird von XPSDaemon nicht unterstützt. Zurzeit werden digitale Zertifikate im Format X.509 Version 3 unterstützt. Dieses Zertifikat kann nicht zur Benutzerauthentisierung verwendet werden.

Aktion: Der Systemadministrator ist über diese Meldung zu informieren.

X030 Startapplikation nicht verfuegbar.

Beschreibung: Die Startapplikation, die in den Sessioneinstellungen ausgewählt wurde, ist nicht verfügbar.

Aktion: Es ist sicherzustellen, dass eine gültige Startapplikation ausgewählt wurde. Wenn dies der Fall ist, ist der Systemadministrator über den Fehler zu informieren.

X034 Der Server verlangt fuer die Anmeldung ein Benutzerzertifikat.

Beschreibung: Für die Anmeldung an den gewählte XPSDaemon Host wird zur Benutzerauthentisierung ein digitales Zertifikat verwendet. Der betroffenen Session wurde kein Zertifikat zugeordnet.

Aktion: Im Rahmen der Sessioneinstellungen ist ein digitales Zertifikat für diese Session auszuwählen. Sollte der Benutzer nicht im Besitz eines zulässigen Zertifikates sein, ist keine Anmeldung an XPSDaemon möglich. In diesem Fall ist der Systemadministrator zu informieren.

X039 Integritaetspruefung fehlgeschlagen.

Beschreibung: Im Rahmen der Integritätsprüfung der übertragenen Daten wurde ein Fehler festgestellt. Die Session wird beendet.

Aktion: Der Systemadministrator ist über diese Meldung zu informieren.

X051 Das virtuelle Terminal ist bereits geöffnet.

Beschreibung: Beim Aufbau einer Session wurde ein virtuelles Terminal verlangt, dass bereits geöffnet ist.

Aktion: Der Session ist ein anderes virtuelles Terminal zuzuordnen.

X053 Die Anzahl der erlaubten Benutzer ist überschritten.

Beschreibung: XPSDaemon lässt das Öffnen weiterer JProtector Sessions nicht mehr zu.

Aktion: Der Systemadministrator ist über den Fehler zu informieren.

Index

3

3270 ..... 13, 42

5

5275 13

A

Applet 13, 19
Arbeitsoberfläche 23
Ausstellerzertifikat 64
Autostart 47

B

Befehlsleiste 23
Benutzerauthentisierung 62
Benutzername 50
Bildschirmmodell 47
Blowfish 38

C

Code Page 80

D

Drag und Drop 79
Drucker 42, 49
Druckersession 42

E

Einfügemarke 50

F

Farbschema 30, 52, 86

H

Host 23, 42, 44, 45, 46, 48
Host Code Page 48
Hostadresse 27, 46
Hosttaste 78, 79

I

IND$-Filetransfer 116
Installation 14

J

Java VM 15

L

Live Update 127

M

Makro 67, 68, 79, 80
Makroname 68
Maskendefinition 121
Maskendefinitionen 29, 30

P

Papierkorb 79
PKCS#12 ..... 38, 53, 62, 63
PKI 62
Popupmenü 24
Portnummer 28

R

Reconnect 47
RSA 39

S

Serverauthentisierung 53, 62
Session 28, 29, 42, 44, 46, 48
Sessionname 28
Sondertaste 79
Sprache 14
Startanwendung 48
Systemadministrator 44
Systeminformation 127

T

Tastaturbelegung 30, 48, 77, 79
TCP/IP 42, 45, 46
TCP/IP Port 46
Telnet 28, 46
Terminalemulation 13, 23, 77
Terminalsession 42

W

Web Start 13, 22

X

XPS Legacy 52
XPSDaemon 23, 28, 46, 48, 127

Z

Zeichensatz 51
Zertifikat 38, 62

Makros

Makros

Makros

Makros